(12) INTERNATIONAL APPLICATION PUBLISHED UNDER THE PATENT COOPERATION TREATY (PCT)

(19) World Intellectual Property Organization
International Bureau

(43) International Publication Date
13 December 2001 (13.12.2001)

PCT

(10) International Publication Number
WO 01/95246 A1

(51) International Patent Classification⁷: G06K 9/00

(21) International Application Number: PCT/US01/18314

(22) International Filing Date: 7 June 2001 (07.06.2001)

(25) Filing Language: English

(26) Publication Language: English

(30) Priority Data:

60/210,270	8 June 2000 (08.06.2000)	US
09/642,459	18 August 2000 (18.08.2000)	US
09/814,607	22 March 2001 (22.03.2001)	US
09/815,568	23 March 2001 (23.03.2001)	US
09/815,885	23 March 2001 (23.03.2001)	US

(71) Applicants and
(72) Inventors: **MURAKAMI, Rick, V.** [US/US]; 596 East 3350 North, North Ogden, UT 84414 (US). **PETTIT, Matthew, W.** [US/US]; 5577 Highland Court, Mountain Green, UT 84050 (US). **GRANT, J., Spencer** [US/US]; 1939 West 420 South, Cedar City, UT 84720 (US). **HINTON, Clark** [US/US]; 5706 North 91 Drive, Glendale, AZ 85305 (US).

(74) Agents: **KRIEGER, Michael, F.** et al.; Kirton & McConkie, 1800 Eagle Gate Tower, 60 East South Temple, Salt Lake City, UT 84111 (US).

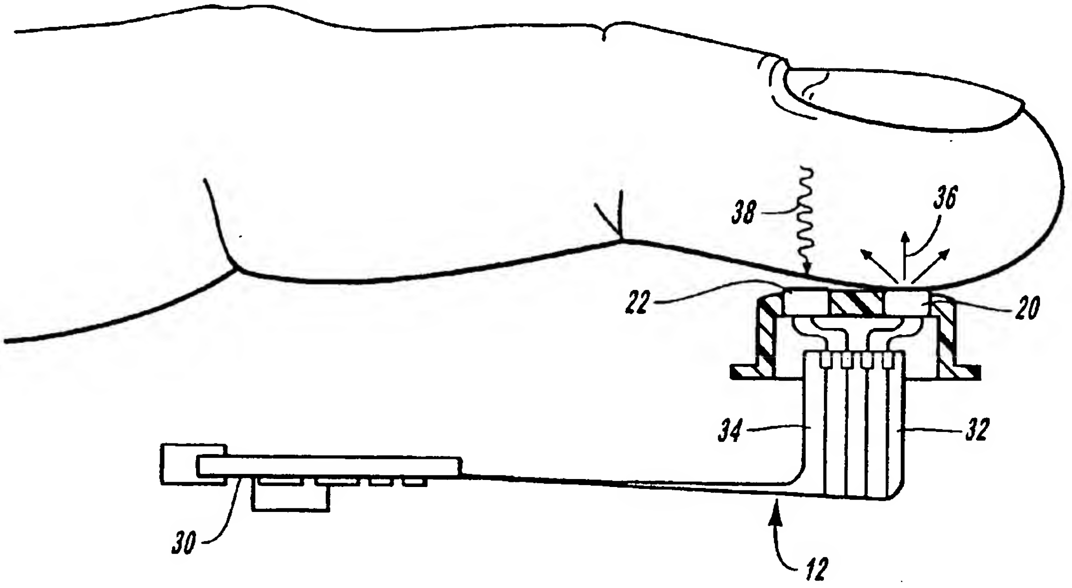
(81) Designated States *(national)*: AE, AG, AL, AM, AT, AU, AZ, BA, BB, BG, BR, BY, BZ, CA, CH, CN, CO, CR, CU, CZ, DE, DK, DM, DZ, EE, ES, FI, GB, GD, GE, GH, GM, HR, HU, ID, IL, IN, IS, JP, KE, KG, KP, KR, KZ, LC, LK, LR, LS, LT, LU, LV, MA, MD, MG, MK, MN, MW, MX, MZ, NO, NZ, PL, PT, RO, RU, SD, SE, SG, SI, SK, SL, TJ, TM, TR, TT, TZ, UA, UG, UZ, VN, YU, ZA, ZW.

(84) Designated States *(regional)*: ARIPO patent (GH, GM, KE, LS, MW, MZ, SD, SL, SZ, TZ, UG, ZW), Eurasian patent (AM, AZ, BY, KG, KZ, MD, RU, TJ, TM), European patent (AT, BE, CH, CY, DE, DK, ES, FI, FR, GB, GR, IE, IT, LU, MC, NL, PT, SE, TR), OAPI patent (BF, BJ, CF, CG, CI, CM, GA, GN, GW, ML, MR, NE, SN, TD, TG).

Published:
— *with international search report*
— *before the expiration of the time limit for amending the claims and to be republished in the event of receipt of amendments*

[Continued on next page]

(54) Title: METHOD AND APPARATUS FOR HISTOLOGICAL AND PHYSIOLOGICAL BIOMETRIC OPERATION AND AUTHENTICATION



(57) **Abstract:** The present invention is directed toward a method and device for biometric authentication using a signal transmitter (20), a signal receiver (22), a memory module, and a processing module. The signal transmitter transmits infrared energy (36) toward a user. The infrared energy is partly absorbed and partly reflected by the user's body. The infra red signal receiver collects partly reflected infrared energy (38). The memory module stores the data, and the processing module processes and compares the reflected infrared energy and stored data for use in biometric authentication.

For two-letter codes and other abbreviations, refer to the "Guidance Notes on Codes and Abbreviations" appearing at the beginning of each regular issue of the PCT Gazette.

METHOD AND APPARATUS FOR HISTOLOGICAL AND PHYSIOLOGICAL BIOMETRIC OPERATION AND AUTHENTICATION

Field of the Invention

The present invention relates to a method and apparatus for activating a device or authenticating a participant in a transaction using histological and/or physiological traits. Specifically, the present invention relates to methods and apparatus employing histological and physiological biometric markers that are substantially unique to an individual in order to permit an individual to activate a device, participate in a transaction, or identify him or herself. More specifically, the present invention relates to methods and apparatus for characterizing and estimating the parameters of a heartbeat signal that is substantially unique to a person in order to permit the person to use the heartbeat signal as a biometric marker to activate a device, participate in a transaction, or identify him or herself.

Background

The computer industry has recognized a growing need for sophisticated security systems for computer and electronic devices. The security systems prevent unauthorized use and authenticate or identify individuals through electronic means. The biometric authentication industry has developed in response to this need. Biometrics is the measurement of quantifiable biological traits. Certain biological traits, such as the unique characteristics of each person's fingerprint, have been measured and compared and found to be unique or substantially unique for each person. These traits are referred to as biometric markers. The computer and electronics industry is developing identification and authentication means that measure and compare certain biometric markers with the intention of using the markers as biological "keys" or "passwords."

Biometric markers presently used by the industry for authentication and identification include the use of measurements of unique visible features such as fingerprints, hand and face geometry, and retinal and iris patterns, as well as the measurement of unique behavioral responses such as the recognition of vocal patterns and the analysis of hand movements. The use of each of these biometric markers requires a device to make the biological measurement and process it in electronic form. The device may measure and compare the unique spacing of the features of a person's face or hand and compare the measured value with a value stored in the device's memory. Where the values match, the person is identified or authorized.

Several types of technologies are used in biometric identification of superficial anatomical traits. For example, biometric fingerprint identification systems may require the individual being identified to place their finger on a visual scanner. The scanner reflects light off of the person's finger and records the way the light is reflected off of the ridges that make up the fingerprint. Hand and face identification systems use scanners or cameras to detect the relative anatomical structure and geometry of the person's face or hand. Different technologies are used for biometric authentication using the person's eye. For retinal scans, a person will place their eye close to or upon a retinal scanning device. The scanning device will scan the retina to form an electronic version of the unique blood vessel pattern in the retina. An iris scan records the unique contrasting patterns of a person's iris.

Still other types of technologies are used for biometric identification of behavioral traits. Voice recognition systems generally use a telephone or microphone to record the voice pattern of the user received. Usually the user will repeat a standard phrase, and the device compares the measured voice pattern to a voice pattern stored in the system. Signature authentication is a more sophisticated approach to the universal use of signatures as authentication. Biometric signature verification not only makes a record of the pattern of the contact between the writing utensil and the recording device, but also measures and records speed and pressure applied in the process of writing.

Each of the prior art systems has a number of disadvantages. For example, fingerprint data bases may raise significant privacy issues for those whose information is entered in the system. Hand and facial geometry recognition systems may require large scanners and/or expensive cameras. Voice recognition devices have problems screening out background noise. Signature recognition devices are subject to variations in the behavior of the individual. Retinal devices may require users to place their eye close to or on a scanning device, exposing the user to potential infection.

Another disadvantage of the prior art to biometric authentication is the limited number of biometric markers that are unique to each individual and that are practical for implementing in computer and electronic devices. Because the biometric patterns used in the prior art to authenticate a person are potentially completely unique to each person, the differences that distinguish one person from another person may be subtle. It may require a high degree of electronic sophistication to read and differentiate between the various unique aspects of the biometric marker. If the biometric marker is used to identify an individual from a large group of individuals, the computer memory storage and processing capability may also have to be sophisticated, and therefore, may be

Another disadvantage of prior art is that with relatively few truly unique biometric markers, it is likely that use of those markers, such as a fingerprint, would be widespread. The widespread use of just one or two types of markers increases the likelihood that an unauthorized person could, by chance or otherwise, be improperly granted access. If an unauthorized person were improperly given access, that individual may have access to numerous secured devices or accounts. This is the same problem that exists when a person chooses the same password for all his accounts or electronic devices.

United States Patent No. 4,537,484 to Fowler et al. discloses a fingerprint imaging apparatus for use in an identity verification system. The system uses light, which is reflected off the finger through a system of mirrors to a linear photo diode ray. The fingers rotated mechanically in order to scan the entire fingerprint.

United States Patent No. 4,544,267 to Shore discloses an identification device that uses a beam of collimated light to scan the fingerprint. The light beam is then imaged onto a linear ray of photo-responsive devices. The information is processed to provide a set of signals containing fingerprint information.

United States Patent No. 4,699,149 to Rice discloses a device for detecting the position of subcutaneous blood vessels such as by using the reflection of incident radiation off of a user's skin. The measured pattern is then compared with a previously determined pattern to verify the identity of the user.

United States Patent No. 4,728,186 to Eguchi et al. discloses another method for detecting data an uneven surface such as a finger, namely a fingerprint, using a light source illuminating the uneven surface through a transparent plate.

United States Patent No. 4,784,484 to Jensen discloses an apparatus for automatic scanning of a fingerprint using an optical scanner. The user slides his finger across a scanning surface and an optical scanning system generates an electrical signal as a function of the movement of the finger across the optical scanning surface.

United States Patent No. 5,073,950 to Colbert et al. discloses a method and apparatus for authenticating and verifying the identity of an individual based on the profile of a hand print using an optical scanner.

United States Patent No. 5,077,803 to Kito et al. discloses a fingerprint collating system employing a biological detecting system.

United States Patent No. 5,088,817 discloses an apparatus for detecting and identifying a biological object by projecting a light beam onto the object and detecting the reflective light using an optical detector. The change in the wave length characteristics of the light beam can be compared to a previously determined pattern.

United States Patent No. 5,230,025 discloses a system for generating data characteristics of a rolled skin print using an optical device that can convert reflective light beams into an electronic signal and generate digital data representative of the image of the skin print.

United States Patent No. 5,335,288 to Faulkner discloses a biometric measuring apparatus that uses silhouette and light images to measure a person's hand features. The features are converted to electronic data and stored and later compared for identification purposes.

Some biometric authentication systems combine biometric measurements with conditions behavior such as signature writing styles and voice patterns or intonations. For example, United States Patent No. 5,103,486 to Grippey discloses a signature verification system utilizing a hand held writing implement that produces data regarding a person's fingerprint pattern and their hand written signature.

Other biometric authentication systems include means for verifying physiological activity. These means for verifying physiological activity are primarily to prevent an unauthorized person from using dead tissues as a means for circumventing the authentication process. For example, United States Patent No. 5,719,950 to Osten et al. discloses a personal biometric authentication system wherein inherently specific biometric parameters are measured and recognized and at least one non-specific biometric parameter is recognized and compared with physiological norms. Likewise, United States Patent No. 5,727,439 to Lapsley et al. discloses an antifraud biometric scanner that determines whether blood flow is taking place in the object being scanned and whether such blood flow is consistent with that of a living human.

One of the difficulties arising from the use of biometric markers for authentication is that the changes that occur in a person's features or physiology over time can alter the measurement of those features and physiology and result in a false negative identification. For example, if a person's facial features are used as a means of biometric identification, and through age or accident the person's features are changed, biometric identification based upon the person's features prior to the change may not be possible. In order to take into account such changes, some biometric authentication systems that rely upon superficial structure or behavioral response have proposed methods for calibrating the authenticating biometric over time.

U.S. Patent No. 5,892,824 to Beatson et al. discloses a biometric template updating process for signature verification, in which an original signature template is modified based on a feature comparison process used in authentication that results in an updated authenticating signature template. U.S. Patent No. 6,111,517 to Atick et al. is which a face recognition biometric device periodically updates the image memory used to authenticate the individual to reflect changes in the appearance of the individual.

The calibration over time of internal physiological and histological markers is complicated by the aging that takes place in the body. The aging process affects the organ systems in the body, which may result in an alteration of the physiological or histological markers. For example, in the integumentary system, as the body ages a degenerative change occurs in collagenous and elastic fibers within the dermis, there is decreased production of pigment in the skin and hair follicles and reduced activity of sweat and sebaceous glands. the body's skin tends to become thinner, more wrinkled and dry with pigmentation spots and the hair becomes gray and ultimately white. Within the skeletal system there is a degenerative loss of matrix, a deterioration of the joints and articulations. bones generally become thinner and more brittle.

Within the muscular system there is a loss of skeletal muscle mass, muscular strength, and motor response. In the circulatory system, the cardiac muscle degenerates and there is decreased diameters of the lumina of the arteries and arterioles, decreased cardiac output, increased resistance to blood flow, and increased blood pressure. With the respiratory system, aging brings on a degenerative loss of elastic fibers in the lungs, a reduced number of functional alveoli, and a reduced vital capacity. Other systems within the body suffer similar degernative effects with aging.

Unlike the calibration issues addressed in superficial biometric markers or behavioral markers, internal physiological and histological markers undergo different kinds of changes. These changes are for the most part invisible and unlike superficial biometric markers, may give no obvious indicia of the change. Likewise, many of the changes in the body systems are largely involuntary responses. These physiological markers do not provide the individual being authenticated an opportunity to try to compensate for whatever changes may occur over time. The changes which occur in internal biometric markers are highly individualized in terms of their timing and degree of change, and therefore may not be compensated for by calibration methods not tailored to the actual changes occurring but are rather predetermined by some other method. Lastly, because internal biometric markers are often combined to form a "compound" biometric marker comprised of a number of physiological and histological features, calibration can be more complicated. In the preferred embodiments of the related applications, multiple features of a physiological event are measured and a select number of the features are used depending on the consistency and distinctiveness of the features. Thus, the features used to authenticate and identify one individual using the system will be different than those features used to identify another individual. With such a system it is important that the calibration techniques take into account the unique nature of the internal biometric marker.

It would also be advantageous to provide a method and apparatus for biometric authentication and activation that does not exclusively rely upon the measurement of superficial anatomical structure and/or behavioral responses and can be calibrated over time. It would also be advantageous to provide a biometric authentication system that is relatively inexpensive and portable. It would be a further advantage to provide a biometric authentication system that can use but does not require the use of truly unique biometric markers where such markers can be calibrated over time. It would also be advantageous to provide a method and apparatus for biometric authentication that can use a single technology to measure multiple, varied biometric markers.

It would therefore be advantageous to provide a method and software for calibrating internal biometric markers and specifically calibrating internal physiological and histological biometric markers over time.

BRIEF SUMMARY OF THE INVENTION

The present invention provides a method and apparatus for identification and authentication using physiological and histological biometric markers. The biometric markers of the present invention are substantially unique to each person, but not necessarily totally unique. The biometric markers of the present invention are not merely measurements of superficial anatomical structure or behavioral traits, but instead utilize or alternatively include measurements of physiological traits of the various systems of the human body and/or are histological traits associated with tissues of the human body. The present invention also contemplates the use of internal biometric markers that are not representative of any particular traits but are a composite of various physiological and/or histological traits. While the biometric markers of the present invention may be entirely unique to each person, markers that are not entirely unique but that are substantially unique may be used in the authentication process. In using substantially unique biometric markers, the present invention also allows a wide variety of biometric characteristics to be employed in a relatively compact and inexpensive device. The present invention employs biological markers that are substantially unique that remain relatively consistent from measurement to measurement and that preferably are capable of being measured without physically invasive procedures.

The present invention provides for the use of a layering technique. The layering technique can enhance the security capabilities of the present invention. Layering is a technique, which employs the use of more than one biometric marker for authentication. Where multiple biometric markers are used to authenticate an unauthorized individual will replicate the authorized person's biometric profile may decrease with the addition of another biometric characteristic to the authentication process.

The present invention may also avoid some of the privacy issues and other disadvantages associated with prior art biometric markers by employing unique physiological or histological biometric markers. For example, use of a physiological marker such as arterial blood pressure is less likely to raise the types of privacy issues associated with the use of fingerprints, does not require expensive scanning equipment, is not subject to behavioral variability, and does not raise issues of undesirable and potentially infectious contact with sensitive tissues.

The use of physiological and histological markers allows the devices in which such a biometric system is used to be both secure and readily manufactured and marketable. Because of the variety of ways in which the physiological markers can be measured and the variety of markers that can be used in the system, the present invention allows for greater flexibility and variability in the design of the device. Prior art systems rely upon the measurement of superficial anatomical structure thereby limiting the application of the associated system. For example, it is in many circumstances financially and technologically impractical to develop a facial or hand recognition system for portable devices such as laptops or PDAs. Contrary to the current trend in the biometric industry, the present invention does not limit the types of markers used to superficial anatomical structure or complex behavioral activity and thus expands the potential applications.

The present invention provides for the use of histological traits of various human tissues. Various kinds of human tissue, such as epithelial tissue, connective tissue, muscle tissue, and nervous tissue, have characteristics which are substantially unique to each person. For example, the depth of the various layers of epithelial tissue from a given point on the skin surface may be a substantially unique histological trait that can be used as a biometric marker. The density of a particular kind of connective tissue, such as bone density, may be a substantially unique histological trait that can be employed in a biometric authentication system. Likewise, the light absorption characteristics of muscle tissue could be a substantially unique histological trait as could the electrical resistance of nervous tissue. The examples given, which are hypothetical and are not intended to be limiting, demonstrate that histologically based biometric markers provide advantages not found in the prior art and in particular, can be used to improve security and increase the variety of applications for which biometric markers are used.

In the same way that histological markers increase both the marketability and security of biometric systems, physiologically based biometric markers also provide advantages for the present invention. Physiological markers do not require the scanning or mapping of anatomical structure. Neither do they require the analysis of volitional acts, as are required with voice or signature analysis. Physiological markers are based upon non-volitional, physiological processes and phenomenon that occur in the body. These markers include physiological processes associated with, but not limited to the (integumentary) system, the skeletal system, the muscular system, the pulmonary system, the respiratory system, the circulatory system, the sensory system, the nervous system, the digestive system, the urinary system, the endocrine system, and the reproductive system. Included in the physiological biometric markers are those activities associated with the various physiological systems that occur automatically or, in other words, are non-volitional. All of these systems and related subsystems provide traits that can be measured in a variety of ways to provide substantially unique biometric markers for the present invention.

Physiological and histological biometric markers may be measured in common units such as spacial measurements of length, area, and volume. Frequency is also another type of measurement that can be practically applied to histological and physiological biometric markers. However, the present invention provides for the monitoring of biometric markers in a variety of other additional ways. The relative motion of particles and fluids can be measured in terms of velocity, acceleration, volumetric flow rate or angular velocity, and angular acceleration. Physical interaction such as force, surface tension, pressure, viscosity, work, and torque are other possible measurements.

The physiological and histological markers may also be based upon energy or heat related characteristics such as power, heat quantity, heat flux, volumetric heat release, heat transfer coefficient, heat capacity, and thermal conductivity. Likewise, measurements, such as electric quantity, electromotive force, electric field strength, electric resistance, and electrical capacities, could provide biometric markers, depending upon the tissue or physiological process being monitored. Magnetic related characteristics, such as magnetic flux, induce, magnetic permeability, magnetic flux density, magnetic field strength, and magneto-motive force could be used. Other potential measurements may include luminous flux, luminance, illumination, radio nucleotide activity, radioactivity, temperature, and absorbed dose and dose equivalent, and amount of substance (mole).

In order to accomplish the present invention, it may be necessary to characterize and estimate the parameters of the physiological/histological markers. Characterization and estimation of the parameters of the physiological/histological marker will be referred to hereinafter as "individualization" of the physiological/histological markers.

The present invention provides an efficient method for employing internal biometric markers. These internal markers can easily be used in conjunction with other biometric techniques to improve the layering technique. The layering technique can enhance the security capabilities of the present invention. Layering is a technique, which employs the use of more than one biometric marker for authentication. For example, the method of the present invention works to greatly simplify the measurement and authentication process, thereby making it more practical to employ layering techniques.

Other physical traits can be used for biometric authentication in conjunction with the individualization of a heartbeat. Where a biometric marker is measured using a signal that passes through these tissues, the tissues may have characteristics that affect the resulting signal or waveform characteristics that are substantially unique to each person. In a preferred embodiment of the present invention, a heartbeat waveform is measured using a signal that passes through dermal and subdermal tissues and their associated vasculature and musculature. Through these tissues the heartbeat of the user is measured and then individualized. The present invention provides for the use of specific histological traits of various human tissues, such as epithelial tissue, connective tissue, muscle tissue, and nervous tissue.

The present invention comprises the steps of obtaining an authenticating or affirmative biometric value from within a range of authenticating biometric values, weighting those values and integrating the values into an authentication data set or template. The biometric values are based upon a measurement of an internal biometric marker, such as an internal physiological or histological biometric marker. The measurement of the internal biometric marker results in a quantitative data set that can then be compared with an authenticating data set for the purposes of biometric identification and authentication. If the data set is confirmed to be authenticating, the data set can be stored electronically then used for purposes of calibration.

The present invention provides a method and apparatus for calibrating physiological and histological biometric markers over time. The biometric markers that are calibrated over time are substantially unique to each person, but not necessarily totally unique. In order to accomplish the present invention, in some cases specified calibration of the physiological/histological markers is necessary. The method of calibration biometric markers of the present invention does not merely calibrate the measurements of superficial anatomical structure or behavioral traits, but can also calibrate internal measurements of physiological traits of the various systems of the human body and/or are histological traits associated with tissues of the human body. These internal traits are calibrated to enhance the traits' capacity to function as a biometric marker. The present invention also contemplates the use of biometric markers that are not a composite of various internal physiological and/or histological traits. While the biometric markers of the present invention may be entirely unique to each person, markers that are not entirely unique but that are substantially unique may be used in the calibration over time and subsequent authentication process. The method of calibration over time of the present invention is capable of calibrating substantially unique biometric markers. The method is easily employed in a relatively compact and inexpensive device. The present invention employs a calibration method for use with biological markers that are substantially unique that remain relatively consistent from measurement to measurement and with markings that preferably are capable of being measured without physically invasive procedures.

The present invention provides an efficient method for employing internal biometric markers that might otherwise be impractical as they change over time. Internal markers that change over time can easily be used in conjunction with other biometric techniques to improve identification and enhance the security capabilities of the biometric identification methods. In particular, the calibration over time method of the present invention can greatly simplify the biometric measurement process.

Using biometric markers that may change over time, a variety of physiological markers can be measured and calibrated allowing for greater flexibility and variability in the markers used and design of the device. Contrary to the current trend in the biometric industry, the present invention does not limit the types of markers used to unchanging superficial anatomical structure or complex behavioral activity, and both simplifies and expands the potential applications for internal markers.

Internal biometric markers may be based upon the traits of human tissue, which could change with time. Various kinds of human tissue, such as epithelial tissue, connective tissue, muscle tissue, and nervous tissue may change and thereby affect biometric characteristics. In a preferred embodiment of the present invention, dermal and subdermal tissues and their associated vasculature and musculature are employed to biometrically identify a user, even though these tissues may be changing over time. Through these tissues a physiological trait, such as the heartbeat of the user, is measured and then calibrated. For example, the depth of the various layers of epithelial tissue from a biometric marker in conjunction with the strength of the heartbeat that also changes. The density of a particular kind of connective tissue, such as bone density, may be a changing histological trait that can be employed as could the light absorption characteristics of skin tissue could be a substantially unique histological trait.

The physiologically based biometric markers that change over time also benefit from the present invention. Specifically, when properly calibrated over time, various characteristics of a heartbeat wave form provide physiological markers that change over time but that do not require the scanning or mapping of anatomical structure. Neither do such heartbeat wave form markers require the analysis of volitional acts, as are required with voice or signature analysis. The present invention takes into account the fact that the heartbeat is a non-volitional, physiological process that occurs within the body. Other physiological processes that change over time can be used including processes associated with, but not limited to, the integumentary system, the skeletal system, the muscular system, the pulmonary system, the respiratory system, the circulatory system, the sensory system, the nervous system, the digestive system, the urinary system, the endocrine system, and the reproductive system. Included in the physiological biometric markers are those activities associated with the various physiological systems that occur automatically or, in other words, are non-volitional. All of these systems and related subsystems provide traits that change over time and that can be measured in a variety of ways to provide unique biometric markers calibrated over time using the present invention.

The method of the present invention for calibrating a biometric marker over a period of time comprises the steps of providing a biometric authentication template, wherein the template includes a set of authenticated biometric measurements. Associated with each measurement is a range of measurement value. To the extent an actual measurement falls within the range of authenticated, measurements, the actual measurement is considered to be an authenticating value. Every authenticating value is averaged into the authentication template, changing the template with each authenticated biometric measurement. A weighted average is used to adjust how much each authenticating measurement changes the template.

In one preferred embodiment, authenticating template is provided using the following process: acquiring a plurality of heartbeats from an individual in an electronic signal form; measuring a plurality of variable features of the electronic signals from the heartbeats; averaging the measurements of each of the signal features; subtracting the average of each measurement from the actual measurement to yield a centroid value; calculate the standard deviation of each measured value; divide the centroid value by the standard deviation for each measured feature to give a T distribution input value;

calculate the probability of the divergence of each measured value using the T-distribution; and input value in a T-distribution analysis.

The probability of divergence can be used to determine whether a subsequently recorded heartbeat signal is characterized by measured features that are significantly different than the template, that is, the authenticating range of measured features. If the measured features are considered "authenticating" when compared to the template, the biometric identification is positive. The measured authenticating features can then be weighted and averaged into the authenticating template, to calibrate the template over time.

In one embodiment, the a global probability that reflects in some way the probabilities for each of the measured features is established, and the global probability is used to compare with subsequently acquired heartbeats. The analysis can be in a univariate, bivariate or multivariate analysis. In bivariate and multivariate analysis, the probability calculations may have to be done using different techniques. A probability analysis for the bivariate may require performing a gamma distribution rather than a t-distribution and may further require the result of the centroid divided by the standard deviation to normalized.

The features can be weighted according to the ability or strength of the measured feature to act as a unique authenticator of a person.

The authenticating biometric measurements, such as an authenticating wave form are weighted before being averaged into the authenticating template. The method by which the authenticating measurements are weighted will depend upon the structure or format of the template. For example, if the template consists of a set of numeric values or range of numeric values associated with particular biometric measurements (such as the rate of a particular physiological process), the biometric measurement may be weighted using a simple multiplier. In this way, one actual biometric measurement will not significantly change the values of the authenticating data set when those measured values are averaged into the authenticating data set but several similar measurements over time can.

The process of weighting various biometric values can be implemented or altered to take into account the likelihood of change over time for a particular biometric marker or feature. Some biometric markers may have rates of change that are more or less universal for all people or the rate of change might be known for a specific individual. Where the rates of change are known, the weighting for those changing biometric markers can be adjusted appropriately. If it is known that a particular feature changes relatively rapidly over time, then greater weight may be given to the authenticating measurements of that feature to allow the calibration to keep pace with the rapidly changing feature.

The weighting may also take into account the relative differences between consecutive authenticating measurements and thereby automatically adjust the weighting for a particular measurement. If it appears that the actual authenticating measurements are consistently lower than the mean measurements in the authenticating template, the weighting of the features may be adjusted accordingly. Where a trend in a change is detected over a series of measurements or a significant departure from previous measurements is recorded, the weighting of the actual measurements may be adjusted as well.

The weighting may also take into account how often the user is employing the biometric authentication device. If there is a significant period of time between biometric measurements the weighting of those authenticating measurements may be adjusted to account for the likelihood of change over that period of time.

The process is carried out on a computerized device, such as any computer system or apparatus employing an electronic processor capable of manipulating data. The process may be embodied in a computer readable medium, such as a software program stored on a disk or drive or may be a computer readable data transmission, such as a propagated signal. The method is presented to a user in a user interface format that facilitates the calibration of the heartbeat signal or waveform.

BRIEF DESCRIPTION OF THE DRAWINGS

The foregoing and other features of the present invention will become more fully apparent from the following description and appended claims, taken in conjunction with the accompanying drawings. Understanding that these drawings depict only typical embodiments of the invention and are, therefore, not to be considered limiting of its scope, the invention will be described and explained with additional specificity and detail through the use of the accompanying drawings in which:

Figure 1 illustrates a front view of an electronic appliance having a biometric authentication device disposed within;

Figure 2 illustrates a transparent front view of the electronic appliance of Fig. 1 revealing the biometric authentication device;

Figure 3 illustrates a cut away side view of the embodiment of Fig. 1;

Figure 4 illustrates a cut away side view of the embodiment of Fig. 1, the electronic appliance is not shown;

Figure 5 illustrates a waveform of the present invention capable of use as a biometric marker;

Figure 6 illustrates a schematic diagram of one embodiment of a transmitter of the present invention; and

Figure 7 illustrates a schematic diagram of one embodiment of a receiver of present invention.

Figure 8 illustrates various features of a waveform;

Figure 9 illustrates a graph showing a strong bivariate relationship; and

Figure 10 illustrates a graph showing a weak bivariate relationship.

Figure 11 illustrates a heartbeat waveform that can serve as one of the biological traits used in the biometric authentication system of the present invention;

Figure 12 illustrates an example of how a heartbeat waveform may be digitally signal processed for use in some embodiments of the present invention; and

Figure 13 shows a diagram of one possible device that may be used in the present invention.

DETAILED DESCRIPTION OF THE PREFERRED EMBODIMENTS

It will be readily understood that the components of the present invention, as generally described and illustrated in the figures herein, could be arranged and designed in a wide variety of different configurations. Thus, the following more detailed description of the embodiments of the system and method of the present invention, and represented in Figures 1 through 7, is not intended to limit the scope of the invention, as claimed, but is merely representative of the presently preferred embodiments of the invention.

The presently preferred embodiments of the invention will be best understood by reference to the drawings, wherein like parts are designated by like numerals throughout.

The various embodiments of the invention will be best understood by reference to the drawings, wherein like elements are designated by like alphanumeric characters throughout. Moreover, it should be noted that because the present invention is computer-implemented, particular embodiments may range from computer executable instructions as part of computer readable media to hardware used to implement the processes herein described. Embodiments of the present invention also include combinations of hardware and computer executable instructions.

Further, whether the invention is described in terms of a method, a system, an application, a type of software, or as computer readable media having computer executable instructions stored thereon, the description is intended to include "instructions" such as program modules, routines, programs, components, data structures, etc. that perform particular tasks within a computing environment. Executable instructions may comprise instructions and data which cause a general purpose computer special purpose computer, or special purpose processing device to perform a certain function or group of functions.

In addition, computer readable media may comprise any available media which can be accessed by a general purpose or special purpose computer. By way of example and not limitation, such computer readable media includes any type of RAM (SDRAM, ESDRAM, etc.) or ROM (EPROM, EEPROM, FEPROM, EAROM, etc.) stored on any physical medium, including a computer chip, a server, or a disk. Disks can include optical storage devices (e.g., CD-ROMs or DVD-ROMs), magnetic storage devices (e.g., floppy disks, Zip® disks, or Bernoulli® cartridges), or any other medium that can be used to store the desired executable instructions or data fields and which can be accessed by a general purpose or special purpose computer. Combinations of any of the above-named media are also included within the scope of computer readable media.

The present invention describes a method and system for biometric access and authentication using histological and physiological traits. The present invention is additionally directed to a method and system for calibrating a biometric marker over time for authentication, using histological and physiological traits.

In a preferred embodiment of the present invention, a biometric marker related to the circulatory system is used to provide authentication and security for a device for transaction. In one preferred embodiment, an infrared light is directed toward a specific part of a user's body, preferably the user's finger. The infrared light penetrates the skin of the finger and is absorbed or reflected off the user's skin and subskin tissues and, specifically, arterial tissues. The reflected light is then received by the system and converted into an electronic signal, which can then be stored in some electronic format.

The changing pressure within the artery or arteries being monitored can be described and analyzed as a hemodynamic waveform. The arterial pressure fluctuates as a result of the cardiac cycle. As the heart's atrium ventricles contract and relax (undergo systole and diastole), pressure in the arterial blood vessels correspondingly rises and falls in a wave-like manner. This pressure waveform has distinct characteristics that result from the timing of systole and diastole and the opening and closing of the cardiac valves. The waveform of one preferred embodiment may be a composite waveform reflecting events in the cardiac cycle, for example: peak systolic pressure, the dicrotic notch, diastolic pressure, the anacrotic notch, and potentially pulse pressure.

In the cardiac cycle, when the right ventricle begins to contract and the pressure in the right ventricle builds, the pulmonic valve opens and blood is passed from the right ventricle into the pulmonary artery, and the pressure in the pulmonary artery naturally increases. As the right ventricle begins to relax, pressure in the pulmonary artery begins to drop. When the pressure in the ventricle declines sufficiently, the pulmonic valve closes and diastole begins. When the pulmonic valve closes, the decline in pressure, as reflected in the waveform, is interrupted by a brief upward movement in the waveform. This interruption is referred to as a dicrotic notch.

Likewise, a dicrotic notch is seen in connection with the aortic valve. When the aortic valve of the heart opens, arterial pressure quickly increases. The arterial pressure increase is the result of the blood flowing out of the left ventricle and into the aorta and arteries. Pressure in the aorta and arterial system continues to rise as blood flows from the left ventricle. As the ventricle completes the contraction, pressure in the aorta begins to decrease and diastole begins. When the aortic valve closes, pressure in the aorta increases temporarily. The closing of the valve and temporary increase in pressure can be seen in graphs of waveforms as a "dicrotic notch."

In the same way the dicrotic notch marks the closing of the pulmonary and aortic valves, the anacrotic notch marks the opening of the aortic valve. As the ventricles enter the systole phase, the rising pressure in the aorta decreases momentarily as a results about the time the aortic valve opens. In the waveform this event is called the anacrotic notch and occurs at the opening of the aortic valve. This notch is generally visible only in central aortic pressure monitoring or in some pathological conditions such as arterial stenosis.

Dicrotic and anacrotic notches reflect the brief change in the waveform that occurs as a result of the opening and closing of the pulmonary and aortic valves. The timing and magnitude of the dicrotic and anacrotic notch is a relatively consistent and substantially unique cardiovascular trait for each person. In the present invention, by monitoring the arterial pressure with an infrared light, a consistent and substantially unique individualized wave pattern can be generated based on the hemodynamic waveform, and in particular, the dicrotic and/or anacrotic notch.

Vasoconstriction of the arteries results in a diastolic pressure. During the period of diastole, blood moves through the larger arteries into smaller arterial branches. The movement of the blood during diastole (such as from the larger to smaller branches) creates some pressure in the arterial system. This pressure is known as diastolic pressure.

Pulse pressure may also be a component of the waveform of the present invention. Pulse pressure represents the difference between the systolic and diastolic pressure. Stroke volume and vascular compliance may also be reflected in the composite wave of the present invention.

In this preferred embodiment of the present invention, the waveform of a user is initially measured and stored in an electronic form. The stored waveform may then be compared to subsequent measured waveforms and, based upon the similarities of the stored waveform and measured waveform, grant or deny access to a device or authorization for transaction. A circulatory biometric marker may be combined with at least one other biometric marker associated with the circulatory system or with another physiological system or histological trait. By "layering" the circulatory biometric marker with at least one other marker, the present invention increases the security of the present invention. In one example of the present invention an electronic apparatus employees and internal biometric marker that is not representative of a particular physiological or anatomical trait.

The means for measuring, recording, and storing the biometric markers employed in the present invention may be any suitable means known in the art. For example, measurement means using absorbed or deflected light rays, and electrical impulses. Means for measuring may include devices capable of measuring pressure differentials, temperature changes, movement, distance, frequency, magnetics, physical interactions, luminescence and radioactivity.

One embodiment of the present invention comprises a signal transmitter and a signal receiver. The signal transmitter transmits energy into dermal and subdermal tissues of the user of a biometric authentication device. The energy transmitted is partly absorbed into the tissues and partly reflected by the tissues. The signal receiver captures the reflected energy and measures the received signal to create a signal profile that represents the absorption and reflection of the signal. The signal data may be collected over any length of time reasonable for authentication purposes. At least one aspect of the data received represents a constant and repeatable characteristic of the signal as absorbed and reflected by the tissues. Furthermore, at least one of the constant and repeatable characteristics is a characteristic that is substantially unique to each person. The resulting constant, repeatable, and substantially unique measurement can be used as a biometric identifier. In one preferred embodiment of a biometric authentication device of the present invention, the signal transmitter emits infrared energy, which is absorbed and reflected by dermal and subdermal layers of a user of the biometric authentication device. The signal transmitter may be an infrared transmitter, such as a light emitting diode, which directs energy into the finger of the user of the biometric authentication device. One embodiment of the present invention is represented by schematic of Figure 6. The IR transmitter transmits at a high energy audio frequency, and is preferably in close proximity to the user's dermal and subdermal tissues. For example, the user may put the user's finger over the light emitting diode in order for the infra red energy to be transmitted into dermal and subdermal tissues and therein be partly absorbed and partly reflected.

The amount of infrared energy that is reflected or absorbed will be partly dependent upon and partly modulated by the anatomical structures and physiological processes taking place within the tissues. Because the anatomical structure and physiological processes of each person will be slightly different, the reflected energy received by the signal receiver will vary from person to person. These structures and processes will uniquely modify the amount of the energy that is absorbed and the amount that is reflected. Many of the structural and physiological differences between individuals will directly affect the absorption and reflection of the energy while others will indirectly affect absorption and reflection. Arterial wall strength, which may vary from individual to individual, creates resistance to blood flow and may affect the timing of the cardiac cycle. Thus, the specific arterial wall strength of an individual user may, because of the structure of the material wall, uniquely modify the signal or, may because of its influence on the flow of blood through the arteries, likewise modify the amount of signal absorbed and the amount reflected. In the case of infrared absorption and reflection of the preferred embodiment, the amount of infrared energy returning to the signal receiver will be modified or modulated by the user's anatomy, such as his or her bone structure, and by physiological processes, such as the user's blood flow. When infrared energy is absorbed and/or reflected by dermal and subdermal tissues, the reflected energy may represent the combined effect of anatomical structures and physiological processes. Thus, the energy received by the signal receiver of the preferred embodiment may be a composite signal that reflects more than just one anatomical structure or physiological process.

In one preferred embodiment of the present invention, the signal receiver is an infrared photo receptor, which receives the infrared energy reflected back from the dermal and subdermal tissues as shown in Figure 7. Biasing techniques, such as biasing transistors, may provide for better reception of the infrared energy signal.

The signal received by the infrared photo receptor is processed, for example, by a processing module, in order for the signal to be stored and used as a biometric identifier. In the preferred embodiment, the photoreceptor receives energy preferably transmitted at high energy audio frequency and conducts this energy signal through a band pass filter, which filters out high and low frequency components of the signal. The signal may be "decreased" using a baseband filter and a low pass filter. Thus processed, the signal is ready to be digitized into a preferable waveform. After being digitized, the signal, now in digital waveform, can be further filtered. Outside present from electric outlets or electrical appliances, can be filtered out and the final digital waveform may be saved. The stored digital waveform will provide the basis for biometric identification.

In a preferred embodiment the signal may be modulated at a higher frequency and then brought back down to a lower base band frequency, which allows the infrared energy to radiate at less power. After the signal is transmitted, the signal can be captured and the low frequency noise filtered out. It is a unique advantage of one embodiment of the present invention to filter out background noise by transmitting the signal that is to be used for biometric identification at a relatively high frequency. The final waveform is stored in a memory module and may represent a composite waveform reflecting anatomical structure and physiological processes, such as blood flow, heart rate, blood pressure, and surrounding bone and blood vessel structure.

The waveform may itself represent a unique biometric marker or may, through a process of layering or applying algorithms to the waveform, yield characteristics substantially unique to each individual and which are constant and repeatable. Some waveforms may need to be "dissected" in order to analyze the various components of the waveform and properly compare waveforms of different users to provide authentication. In the preferred embodiment, the waveform is primarily associated with cardiovascular processes in the body, however, the waveform could represent any one or more of the body's internal physiological processes or anatomical structures.

Anticipating that the physiological and anatomical attributes of a user of the present invention will change over time, the present invention provides for a method of self-calibration. Self-calibration allows the stored, authenticating signal or waveform to be modified to coincide with the changes in the user's physiological and anatomical attributes over time. For example, if the authentication system involves monitoring cardiovascular function, the user's heart function changes with time and the signal received from the authorized user may also slightly change over time. Thus, the authorized user's signal may be slightly different from the originally stored, authenticating signal.

In order to allow for the changes that occur in the user's body, the authentication program of the present invention provides for some degree of variance between the stored, authenticating waveform and an authorized user's waveform. The program can track such variances over time and modify the stored authenticating waveform to more closely match the slightly changed waveform of the authorized user, if necessary. Self-calibration allows the authenticating signal to be modified within a statistical limit, to and insubstantial changes in the authorized user's waveform increase over time, the authenticating signal can also be changed. Self-calibration may be applied by the use of a calibration program and is preferably an automatic and continuous calibration that is performed upon each use of the authentication device.

When a received signal is compared to an authenticating signal, if the signals or waveforms are statistically identical, the present invention will transmit a validating signal, which may activate a switch or otherwise enable a device. Where the signals or waveforms are not statistically identical, a signal indicating the waveform is "invalid" is generated. When the signal is not valid, the biometrically activated switch will remain off or the device will remain disabled.

In one preferred embodiment, the signal transmitter and the signal receiver constitute an infrared light emitting diode placed in an on/off button for a biometrically activated device. The signal receiver can be a photoreceptor connected to a single chip solution and integrated into PCA of a portable electronic device. The photoreceptor may be located in the same plane as the LED and may be positioned relatively near to the transmitter. For example, in one embodiment, the photoreceptor is embedded in the same on/off button as the LED and is approximately a quarter inch away from the LED.

Figure 1 illustrates an electronic appliance 10 having a biometric authentication device 12. A biometric authentication device comprises a button 26 or switch 26 for enabling the electronic appliance 10, in this case as mobile phone. The biometric authentication device 12 is incorporated into the power button 26 of the phone so that the signal transmitter 20 and the signal receiver 22 are in the same plane and are proximate to each other. Figure 2 shows the biometric authentication device 12 being connected to a single chip 30 that is integrated into the PCA of the phone 10. The signal transmitter 20 is connected to the chip 30 through transmitter wires 32 and the signal receiver is connected to the chip through receiver wires 34.

The signal transmitter 20 can be any transmitter known or used in the art capable of transmitting energy into dermal and subdermal layers such that the energy signal is partly absorbed and/or partly reflected back toward the signal receiver 22. The signal receiver 22 can likewise be any device capable of receiving the partly reflected signal. In the preferred embodiment of the present invention, as shown in Figure 2, the preferred signal transmitter 20 is an infrared light emitting diode and the preferred signal receiver 26 is a photoreceptor.

Figure 3 shows a side view of the present invention with a signal receiver 20 and a signal transmitter 22 being connected to receiver wires 34 and transmitter wires 32 leading to the chip 30. The signal receiver 22 and signal transmitter 30 are embedded in the button 26, which is disposed in the phone 10.

Figure 4 illustrates a user's finger absorbing energy from the signal transmitter 20 and receiving reflected energy from the dermal and subdermal tissues of the user's finger in the signal receiver 22.

The signal transmitter 20 is activated by the placement of the finger on the button 26. The signal transmitter 20 is preferably activated when the user places his or her finger on the button 26. The signal transmitter 20 may be activated by pressure from the user's finger, by an optical switch, motion detector, or heat sensor, or any other means for activation. When the signal transmitter 20 is activated, a signal 36 is emitted from the signal transmitter 20 and is transmitted into the user's dermal and subdermal tissues. The signal 36 is partly absorbed and partially reflected by the dermal and subdermal tissues. The reflected signal 38 is received by a signal receiver 22 and transmitted through receiving wires 34 to the chip 30. Within the chip 30, the received signal 38 is processed and transformed into a biometric identifier such as a digital waveform shown in Figure 5. The biometric identifier is then compared to the stored, authenticating biometric identifier. If the received biometric identifier is the same as the stored, authenticating biometric identifier, the device 10 is enabled.

Example 1

In a preferred embodiment of the present invention, a biometric authentication system uses multiple biometric markers for authentication in a transaction. Using an infrared reading device comprising a signal transmitter and a signal receiver both connected to a processing module and a memory module, biometric markers based upon a composite waveform are taken. In alternative embodiments, different cardiovascular related biomarkers are measured. The biometric profile based upon the composite waveform is created and stored in the device. When a user wishes to authenticate his participation in a transaction, the user places his finger on the infrared reading device allowing the system to obtain measurements on the biometric markers. The biometric markers are processed and compared to those stored. Where the biometric markers match the individual is able to authenticate his participation in the transaction.

Example 2

In one embodiment of the present invention, a biometric authentication system is provided to control access or to authenticate. The system comprises electronically recording biometric markers using an electronic recording instrument. The electronic recording instrument measures at least one biometric marker. The measured trait is capable of acting as a biometric marker because it is selected from the traits that are substantially unique. If a trait or measurement taken from one individual has only at least approximately a one in two chance of being the same as the measurement of that same physical trait taken from another person the trait is substantially unique. The trait is also a trait that is substantially consistent when measured for the same person and is preferably capable of being measured in a noninvasive method. The trait is a trait associated with the integumentary system.

Use of the integumentary system in the biometric authentication system of this embodiment provides relatively easy access to the biometric markers, since the integumentary system is relatively superficial as compared to other systems. The integumentary system also provides an effective line of defense against infection. Thus, if a biometric authentication system requires several users to come into contact with the biometric system, the integumentary system acts as a barrier to the passing of infection whereas other tissues may not provide such a barrier. Moreover, the integumentary system provides several layers of integument from which biometric markers can be taken. Glandular activity of the integument and other epidermal derivatives such as hair and nails may also supply biometric markers for use with this exemplary embodiment of the present invention.

After measuring at least one biometric marker, the marker is recorded electronically and stored to constitute a biometric profile of the person. The information stored as a biometric profile is preferably stored in the portable device, or is at least available to the portable device upon demand. In the preferred embodiment, more than one biometric marker is measured and recorded to constitute a multi-marker biometric profile.

The information stored as a biometric profile is then designated as an authenticating profile. In other words, the stored profile will act as a password, preventing access to the device unless a substantially identical biometric profile is measured by the device. The device is designed so that before the device is fully activated, the device must measure and compare a user's biometric profile with the authorized biometric profile. If the biometric profile measured is substantially identical to the stored biometric profile, then the user may be granted access to the device.

Example 3

In one embodiment of the present invention, a biometric authentication system is provided to control access or to authenticate. The system comprises electronically recording biometric markers using an electronic recording instrument. The electronic recording instrument measures at least one biometric marker. The measured trait is capable of acting as a biometric marker because it is selected from the traits that are substantially unique. The trait is also a trait that is substantially consistent when measured for the same person and is preferably capable of being measured in a noninvasive method. The trait is a trait associated with the skeletal system.

Use of the skeletal system in this embodiment of the present invention provides a relatively stable and relatively unchanging system from which biometric markers can be taken. The variety of tissues and structures and various physiological processes associated with the skeletal system and articulating joints may provide multiple biometric markers with this preferred embodiment. For example, biometric markers related to ligament layering may be found to be effective biometric markers.

After measuring at least one biometric marker, the marker is recorded electronically and stored to constitute a biometric profile of the person. The information stored as a biometric profile is preferably stored in the portable device, or is at least available to the portable device upon demand. In the preferred embodiment, more than one biometric marker is measured and recorded to constitute a multi-marker biometric profile.

The information stored as a biometric profile is then designated as an authenticating profile. The device is designed so that before the device is fully activated, the device must measure and compare a user's biometric profile with the authorized biometric profile. If the biometric profile measured is substantially identical to the stored biometric profile, then the user may be granted access to the device.

Example 4

In one embodiment of the present invention, a biometric authentication system is provided to control access or to authenticate. The system comprises electronically recording biometric markers using an electronic recording instrument. The electronic recording instrument measures at least one biometric marker. The measured trait is capable of acting as a biometric marker because it is selected from the traits that are substantially unique, in other words the trait measurement taken from one individual has only at least a one in two chance of being the same as the measurement of that same physical trait taken from another person. The trait is also a trait that is substantially consistent when measured for the same person and is preferably capable of being measured in a noninvasive method. The trait is a trait associated with the muscular system.

Use of the muscular system in this preferred embodiment of a biometric authentication device may provide numerous potential biometric markers because of the highly specific and specialized function of the various muscles in the muscular system. For example, the human hand is an extremely complex portion of the muscular

This complex system allows for intricate movement of the hand in response to various stimuli. It is believed that substantially unique biometric markers relating to the muscular system, and in particular to the muscular system of the hand, exist. For example, the duration of action potentials and their effect on a particular muscle may be a potential biometric marker that can be used in this preferred embodiment of the present invention.

After measuring at least one biometric marker, the marker is recorded electronically and stored to constitute a biometric profile of the person. The information stored as a biometric profile is preferably stored in the portable device, or is at least available to the portable device upon demand. In the preferred embodiment, more than one biometric marker is measured and recorded to constitute a multi-marker biometric profile.

The information stored as a biometric profile is then designated as an authenticating profile.

The device is designed so that before the device is fully activated, the device must measure and compare a user's biometric profile with the authorized biometric profile. If the biometric profile measured is substantially identical to the stored biometric profile, then the user may be granted access to the device.

Example 5

In one embodiment of the present invention, a biometric authentication system is provided to control access or to authenticate. The system comprises electronically recording biometric markers using an electronic recording instrument. The electronic recording instrument measures at least one biometric marker. The measured trait is capable of acting as a biometric marker because it is selected from the traits that are substantially unique. The trait is also a trait that is substantially consistent when measured for the same person and is preferably capable of being measured in a noninvasive method. The trait is a trait associated with the respiratory system.

The respiratory system provides a relatively consistent and systematic physiological process to be monitored, particularly as it relates to pulmonary activity and the supply of oxygen and removal of carbon dioxide from the blood stream. Respiratory activity in many instances can be easily monitored. The inventors believe that there are multiple respiratory characteristics that are substantially unique to each individual and that such characteristics may be employed in a biometric authentication system. For example, measurements relating to O_2 and CO_2 content in various tissues may be found to be suitable as a biometric marker.

After measuring at least one biometric marker, the marker is recorded electronically and stored to constitute a biometric profile of the person. The information stored as a biometric profile is preferably stored in the portable device, or is at least available to the portable device upon demand. In the preferred embodiment, more than one biometric marker is measured and recorded to constitute a multi-marker biometric profile.

The information stored as a biometric profile is then designated as an authenticating profile. The device is designed so that before the device is fully activated, the device must measure and compare a user's biometric profile with the authorized biometric profile. If the biometric profile measured is substantially identical to the stored biometric profile, then the user may be granted access to the device.

Example 6

In one embodiment of the present invention, a biometric authentication system is provided to control access or to authenticate. The system comprises electronically recording biometric markers using an electronic recording instrument. The electronic recording instrument measures at least one biometric marker. The measured trait is capable of acting as a biometric marker because it is substantially unique. The trait is also a trait that is substantially consistent when measured for the same person and is preferably capable of being measured in a noninvasive method. The trait is a trait associated with the cardiovascular system.

Because of the remarkable ability of the heart to continually and rhythmatically pump blood through the cardiovascular system, the cardiovascular system provides numerous biometric markers for use in this preferred embodiment. The cardiac cycle alone as explained above in Example 1, undergoes both an electrical and physical phenomena that result in potential biometric markers. The fluid dynamics of the vascular system also provide potential biometric markers.

After measuring at least one biometric marker, the marker is recorded electronically and stored to constitute a biometric profile of the person. The information stored as a biometric profile is preferably stored in the portable device, or is at least available to the portable device upon demand. In the preferred embodiment, more than one biometric marker is measured and recorded to constitute a multi-marker biometric profile.

The information stored as a biometric profile is then designated as an authenticating profile. The device is designed so that before the device is fully activated, the device must measure and compare a user's biometric profile with the authorized biometric profile. If the biometric profile measured is substantially identical to the stored biometric profile, then the user may be granted access to the device.

Example 7

In one embodiment of the present invention, a biometric authentication system is provided to control access or to authenticate. The system comprises electronically recording biometric markers using an electronic recording instrument. The electronic recording instrument measures at least one biometric marker. The measured trait is capable of acting as a biometric marker because it is substantially unique. The trait is also a trait that is substantially consistent when measured for the same person and is preferably capable of being measured in a noninvasive method. The trait is a trait associated with the sensory system.

Use of the sensory system as a source for biometric markers provides a number of highly specialized reactions that can be readily tested. This is because the sensory system is specifically designed to receive stimuli from the external environment. For example, the dilatory response of the eye to a certain amount of light may provide a potential biometric marker.

After measuring at least one biometric marker, the marker is recorded electronically and stored to constitute a biometric profile of the person. The information stored as a biometric profile is preferably stored in the portable device, or is at least available to the portable device upon demand. In the preferred embodiment, more than one biometric marker is measured and recorded to constitute a multi-marker biometric profile.

The information stored as a biometric profile is then designated as an authenticating profile. The device is designed so that before the device is fully activated, the device must measure and compare a user's biometric profile with the authorized biometric profile. If the biometric profile measured is substantially identical to the stored biometric profile, then the user may be granted access to the device.

Example 8

In one embodiment of the present invention, a biometric authentication system is provided to control access or to authenticate. The system comprises electronically recording biometric markers using an electronic recording instrument. The electronic recording instrument measures at least one biometric marker. The measured trait is capable of acting as a biometric marker because it is substantially unique. The trait is also a trait that is substantially consistent when measured for the same person and is preferably capable of being measured in a noninvasive method. The trait is a trait associated with the nervous system.

Because of the anatomically ubiquitous nature of the nervous system, and its markers that may be used in this embodiment. For example, the response of a particular nerve or bundle of nerves to a measured electrical stimulus may provide a biometric marker for use in this embodiment.

After measuring at least one biometric marker, the marker is recorded electronically and stored to constitute a biometric profile of the person. The information stored as a biometric profile is preferably stored in the portable device, or is at least available to the portable device upon demand. In the preferred embodiment, more than one biometric marker is measured and recorded to constitute a multi-marker biometric profile.

The information stored as a biometric profile is then designated as an authenticating profile. The device is designed so that before the device is fully activated, the device must measure and compare a user's biometric profile with the authorized biometric profile. If the biometric profile measured is substantially identical to the stored biometric profile, then the user may be granted access to the device.

Example 9

In one embodiment of the present invention, a biometric authentication system is provided to control access or to authenticate. The system comprises electronically recording biometric markers using an electronic recording instrument. The electronic recording instrument measures at least one biometric marker. The measured trait is capable of acting as a biometric marker because it is substantially unique. The trait is also a trait that is substantially consistent when measured for the same person and is preferably capable of being measured in a noninvasive method. The trait is a trait associated with a metabolic system.

The numerous metabolic processes of the body provide a number of biometric markers for use in the present invention. For example, the ability of certain tissues to absorb or release heat over time and the body's ability generally to control internal temperatures may provide a biometric marker.

After measuring at least one biometric marker, the marker is recorded electronically and stored to constitute a biometric profile of the person. The information stored as a biometric profile is preferably stored in the portable device, or is at least available to the portable device upon demand. In the preferred embodiment, more than one biometric marker is measured and recorded to constitute a multi-marker biometric profile.

The information stored as a biometric profile is then designated as an authenticating profile. The device is designed so that before the device is fully activated, the device must measure and compare a user's biometric profile with the authorized biometric profile. If the biometric profile measured is substantially identical to the stored biometric profile, then the user may be granted access to the device.

Example 10

In one embodiment of the present invention, a biometric authentication system is provided to control access or to authenticate. The system comprises electronically recording biometric markers using an electronic recording instrument. The electronic recording instrument measures at least one biometric marker. The measured trait is capable of acting as a biometric marker because it is substantially unique. The trait is also a trait that is substantially consistent when measured for the same person and is preferably capable of being measured in a noninvasive method. The trait is a trait associated with the dicrotic notch and/or anacrotic notch of a person's hemodynamic waveform.

After measuring at least one biometric marker, the marker is recorded electronically and stored to constitute a biometric profile of the person. The information stored as a biometric profile is preferably stored in the portable device, or is at least available to the portable device upon demand. In the preferred embodiment, other biometric markers are measured and recorded to constitute a multi-marker biometric profile.

The information stored as a biometric profile is then designated as an authenticating profile. The device is designed so that before the device is fully activated, the device must measure and compare a user's biometric profile with the authorized biometric profile. If the biometric profile measured is substantially identical to the stored biometric profile, then the user may be granted access to the device.

Example 11

In one embodiment of the present invention, a biometric authentication system is provided to control access or to authenticate. The system comprises electronically recording biometric markers using an electronic recording instrument. The electronic recording instrument measures at least one biometric marker. The measured trait is capable of acting as a biometric marker because it is substantially unique. The trait is also a trait that is substantially consistent when measured for the same person and is preferably capable of being measured in a noninvasive method. The trait is a trait associated with the anacrotic notch of a person's cardiac waveform.

After measuring at least one biometric marker, the marker is recorded electronically and stored to constitute a biometric profile of the person. The information stored as a biometric profile is preferably stored in the portable device, or is at least biometric markers are measured and recorded to constitute a multi-marker biometric profile.

The information stored as a biometric profile is then designated as an authenticating profile. The device is designed so that before the device is fully activated, the device must measure and compare a user's biometric profile with the authorized biometric profile. If the biometric profile measured is substantially identical to the stored biometric profile, then the user may be granted access to the device.

Example 12

In one embodiment of the present invention, a biometric authentication system is provided to control access or to authenticate. The system comprises electronically recording biometric markers using an electronic recording instrument. The electronic recording instrument measures at least one biometric marker. The measured trait is capable of acting as a biometric marker because it is selected from the traits that are substantially unique, in other words the trait measurement taken from one individual has only at least a one in two chance of being the same as the measurement of that same physical trait taken from another person. The trait is also a trait that is substantially consistent when measured for the same person and is preferably capable of being measured in a noninvasive method. The trait is a trait associated with cardiovascular processes as exhibited in a person's finger.

After measuring at least one biometric marker, the marker is recorded electronically and stored to constitute a biometric profile of the person. The information stored as a biometric profile is preferably stored in the portable device, or is at least available to the portable device upon demand. In the preferred embodiment, other biometric markers are measured and recorded to constitute a multi-marker biometric profile.

The information stored as a biometric profile is then designated as an authenticating profile. In other words, the stored profile will act as a password preventing access to the device unless a substantially identical biometric profile is measured by the device.

The device is designed so that before the device is fully activated, the device must measure and compare a user's biometric profile with the authorized biometric profile. If the biometric profile measured is substantially identical to the stored biometric profile, then the user may be granted access to the device.

Example 13

In another example of the present invention, the biometric device is used to grant access to a personal computer or some similar electronic device. In this example, the signal transmitter is built into the keyboard, mouse, tower or monitor of the personal computer. The signal transmitter may be activated by turning on the computer and activating the transmitter the transmitter or the transmitter may itself regulate the power supply to the computer. The signal transmitter sends energy into dermal and subdermal tissues of the user of a biometric authentication device. For example, the user may place his or her finger onto the transmitter located on mouse in which the present invention is disposed. The energy transmitted is partly absorbed into the tissues of the finger and partly reflected by the tissues. The signal receiver then captures the reflected energy and measures the received signal to create a biometric profile.

When the biometric profile matches the authorized biometric profile, the author is granted access to the use the computer, access certain data, or run an application. The storage and processing power of the computer may be utilized to facilitate the biometric identification procedure.

Heartbeat Waveforms

In one preferred embodiment, the present invention monitors the actual waveform of the heartbeat and retains certain features or attributes associated with that waveform for use in individualization and authentication. For example, the position on the upslope of the heartbeat waveform having the fastest rate of change slope can be recorded and various attributes of that position can be noted. The amplitude of that position, its position from the center of the pulse and amplitude of the actual beat relative to the position can all be measured and recorded. Thus, multiple quantitative features can be extracted from a single characteristic of a waveform.

All of the heartbeat waveforms share a number of standard features that can be used as reference points for other measurements. For example, all heartbeat waveforms can be divided into two distinct peaks. As part of the individualization process, the heartbeat waveform can be analyzed relative to the two peaks. Various parameters associated with waveform peaks include, but are not limited to, the differences between the two peak amplitudes, the differences between the two peak rate of changes, the relative position of the dicrotic notch, how deep the notch is, how far the dicrotic notch is from a zero point--a reference point, and how far it is from the center of one of the peaks, where the peak of the dicrotic notch is located along the horizontal, and the position of the various peaks from the center of the waveform and from the center of the other peak. Often several features can be extracted out of the waveform to serve in the individualization process.

Features of the heartbeat wave form that could be used for authentication include but are not limited to:
Rate of change (slope) at all locations of the wave form. (There are n-1 of these per wave form. n= number of data points)
Shape of Peak associated with the strongest wave form feature
Shape of Peak associated with the dicrotic notch
Shape of Inverted Peak associated with dicrotic notch
Approach angle of Peak associated with the strongest wave form feature
Approach angle of Peak associated with the dicrotic notch
Approach angle of Inverted Peak associated with the strongest wave form feature
Approach angle of Inverted Peak associated with dicrotic notch
Location of Peak associated with the strongest wave form feature
Relative location of Peak associated with the strongest wave form feature
Location of Peak associated with the dicrotic notch
Relative location of Peak associated with the dicrotic notch
Location of Inverted Peak associated with the dicrotic notch
Relative Location of Inverted Peak associated with the dicrotic notch
Magnitude of Peak associated with the strongest wave form feature
Magnitude of Peak associated with the dicrotic notch
Magnitude of Inverted Peak associated with dicrotic notch
Maximum rates of change along any defined segment of the wave form
Minimum rates of change along any defined segment of the wave form
Relative location associated with maximum rates of change along any defined segment of the wave form
Relative location associated with minimum rates of change along any defined segment of the wave form
Magnitude associated with maximum rates of change along a defined segment of the wave form
Magnitude associated with minimum rates of change along any defined segment of the wave form
Frequency of the wave form as determined by any data point
Frequency of wave form as determined by a combination of data points

Features of the heartbeat wave form that could be used for authentication include but are not limited to:
Trend measures associated with a feature
Trend measures associated with any segment and wave form
Cycles associated with any feature
Cycles associated with any segment of the wave form
Series associated with a feature
Series associated with a segment of the wave form
Variability estimates associated with features
Variability estimates associated with subsegments
Variability estimates associated with defined measures
Linear combination of features, segments, and data on a wave form
Non-linear combinations of features, segments, and data on a wave form

In another example, shown in Figure 8, various features of the waveform are monitored, such as peaks in the waveform, for quadratic and linear comparison. At the peak of the heartbeat, the waveform can be analyzed to show a quadratic fit. The quadratic term and the linear term of the quadratic that most closely correspond to the curve across the top of that heartbeat are potential features of the waveform that can be used for identification. Likewise, other features shown in Figure 8 as well as those listed in Table A may prove useful in using the waveform as a biometric marker.

In a preferred embodiment, a total of 25 features are extracted out of a waveform to create a list of 25 parameters, each parameter representing a different unique feature for a particular person's heartbeat waveform. In addition to the selected heartbeat waveform parameters, other internal biometric features which are not related to a heartbeat waveform can be included in the list of parameters used in identification. For example, a measurement of the skin's light conductance may not be related to the heartbeat waveform and is a different kind of parameter, but light conductance can be easily measured in conjunction with the capture of the heartbeat waveform. These various features are ideally measured at the same time and can create very powerful identification multipliers since the features may vary over a wide range of individuals.

In order to individualize an internal biometric identifier such as a heartbeat waveform, the biometric must be read and recorded at least once. In order to assure an accurate biometric, it is preferable to take more than one reading of the biometric for purposes of individualization. In one preferred embodiment 30 heartbeats were taken and monitored to do the individualization for each person being identified. In another preferred embodiment, a hundred heartbeats were used. In capturing a good sample, it is preferred to take as many samples as is possible. However, taking a large number of sample waveforms takes time and using an extended period of time to individualize the waveform may be impractical.

Having collected various heartbeat waveforms from a person and determined various feature's measurements for each waveform, a table of extracted waveform features measurements can be created. The information in the table is used to individualize the waveforms of the person from whom the measurements were collected into a biometric authenticator.

The first step in the individualization process is determining the mean vector of the measured features in the table. For each feature on the table, the average of all the samples of that feature is calculated and then the average of that feature measurement is subtracted out from the actual measurement of the feature. The difference yields a value called the "centroid value" or "centroid vector" of the feature measurement.

Next, the standard deviation for each feature measurement is calculated, to show the degree statistical variation the waveforms have among themselves. Where there is little fluctuation or variation in a measured feature of the waveforms, the feature is relatively consistent and may be a good authenticating feature and the standard deviation is low. If there is significant variation in the waveform, the standard deviation is high.

Next, each of the measured features is subjected to a probability calculation. In one embodiment, using the centroidal information, the probability that a particular sample would exist given the range of measurements taken for that particular feature is determined. A valid sample is one that falls within a desired range of measurements. For any given sample, the probability calculation determines how closely that feature's measured value corresponds to the measurements of that same feature on other waveforms from that person. Where the measurements for the features of two waveforms are consistent and close together, the range of values for the measurement and related probabilities for the occurrence of that value can be determined. A subsequent measurement that shows up within that a range of values that have a high probability of occurrence is a "valid" measurement. In other words, there is a good probability that the subsequently generated waveform could come from the person whose waveform generated the initial data set. In one preferred embodiment, the probability for each measurement is calculated using a T distribution and the centroid value and the standard deviation.

Before running the T-distribution, it is necessary to take into account the fact that for some of the features, the variation can be very rare, while for others, variations could be quite common. In order to individualize the values, the centroid value for each measurement is divided by the standard deviation. By individualizing of each one of the data samples, all the data samples will be in the same standard set regardless of the feature.

After the data are individualized, they are used to carry out the T distribution to generate corresponding probabilities for the measured values. Using these probability figures, a "threshold" value for each particular feature is determined, that is, the lowest acceptable probability value is determined. In one preferred embodiment the minimum univariate value is used as the threshold for determining whether the measurement taken of a particular feature is considered within the range of acceptable variance or is outside the acceptable range. The values calculated from an individual for whom the waveform is being individualized should fall above the minimum univariate value.

Obviously, it is possible that two people will have one or more waveform features so similar that the values taken from one will match or correspond to the other. If only one feature of the waveform were measured and individualized for the purposes of biometric authentication, then there is a strong possibility that two different people would have similar measured values for their "biometric profiles." In order to reduce the likelihood of such false positives, calculations are carried out for multiple features creating a table of univariates with corresponding minimum values. These minimum values can be compared or combined to yield an overall or global minimum univariate event called the total minimum.

The various data collected from the waveform and generated from the calculations performed on the collected waveform create a data set unique to person from whom the data were gathered. By combining the probabilities to create a univariate threshold, the present invention creates a unique biometric marker from a data set taken from an internal biometric marker.

In addition to univariate processing, the present invention also provides for bivariate processing. Bivariate processing begins with a determination of whether a relationship exists between the values for each of the features. For example, a determination must be made as to whether there is a correlation between feature one and feature two. If one feature represents amplitude of the waveform and a second feature is the amplitude of the dicrotic notch, and the two features measurements correspond in some reliable way, (e.g., the depth of the dicrotic notch is deep when the width of the pulse is narrow) the relationship can be used to further individualize the waveform to function as a biometric marker.

If there is a strong relationship between two univariate values, a linear correlation may exist and be used to individualize the waveform. The linear relation between the features can be shown graphically by taking the measured values and plotting it with the other related, measured values. Where the relationship between the values is strong, the graph has a cigar shape, as shown in Figure 9, but where the relationship is not as strong, the graph would has a round shape instead, as shown in Figure 10. In order to determine how well the features correlate with each other, each possible pairwise combination of features is evaluated. In the preferred embodiment having 25 features there are 300 possible bivariates. All 300 are analyzed for purposes of individualization .

In order to evaluate the degree of correspondence between two variables, the centroid value for each measurement of each measured feature is divided by its standard deviation and then multiplied together. The resulting values are summed and the summation is divided by the degrees of freedom (a value one less than the number of samples in the summation).

By comparing the bivariate combinations, a determination can be made as to which bivariates have the highest degree of correspondence. In some circumstances a user may have two different univariate values that individually are too inconsistent to function as validators, but show a strong correlation between their otherwise inconsistent values. These two "individually weak" univariates can be combined to form a strong bivariate. Using the summation calculation above, one can determine which bivariates have a strong correspondence. Bivariates that correspond exactly have a summation value of one. Where there is no correspondence at all, the summation value is zero. Bivariates with a correspondence close to one are typically the most helpful in individualizing the waveform and in subsequent authentication.

Having performed summation on a selected group of bivariates, a threshold value between zero and one is applied to the summation of the group. The selection of the threshold value is determined by balancing the need for highly correlating bivariates versus the need to employ a large number of bivariates. For example, a threshold value of 0.8 may be selected for a given group of bivariate. If the summation value of a particular bivariate is less than 0.8 then that bivariate value is not included in the biometric individualization, if it is above 0.8, then the bivariate correlates to an acceptable degree and the bivariate is included in the biometric individualization. Each one of these bivariates having a summation that falls above the 0.8 threshold value is electronically flagged and stored to be used as part of the individualization

The number of bivariates that will be used in the individualization will depend upon the threshold values chosen and also on the individual for whom the individualization is done. Likewise the bivariates chosen will change from person to person because the bivariate correlation will change; some of the bivariates will work better for some people than they will for others. However, after the bivariates are established for a given person, the same bivariates are used for subsequent authentication.

Next the probability of the bivariates are calculated. In order to determine the probability that two bivariates properly authenticate the user, the Mahalanobis distance of the each of the bivariates is calculated. Determining this Mahalanobis distance involves calculating the average of the bivariates and determining the difference of each value from the average. Then using a cumulative gamma distribution calculation for each of the measured Mahalanobis distances, the probability that a certain bivariate represents the authentic user is calculated.

Comparing all of the univariate and bivariate probabilities, the minimum probability minimum value for all is obtained. The minimum probability can be used as threshold or basis for indicating identity between a present user's biometric "signature" and the signature as initially individualized. Alternatively, the probability value is just above the minimum value or some other probability value can be used.

All the information gathered and calculated by these various processes can be stored for use in individualization, calculations and verifications. The data is stored as the processes are completed. For example, for each feature, the measured value, the average, the centroid, the standard deviation, the minimum univariate T distribution, and the bivariates gamma distribution are stored in the device for later use.

In summary, the process of individualizing a person's heartbeat waveform under normal operations comprises the steps of capturing and saving the heartbeat signal, measuring particular features of the signal, subtracting each measurement from the average to yield the centroid, then, dividing each centroid by the standard deviation as calculated using the individualization set, determining the probability of the resulting figure using a distribution calculation and comparing the probability to the minimum value established. If the values are within the limits established by the individualization set, the person is authenticated. Using the data from the signal, a set of highly correlating bivariates is defined and distribution calculations are performed to determine the probability of the measured bivariates. The bivariate probabilities are also used in individualization and subsequent authentication.

One problem in making such authentication is knowing how to establish a the minimum probability is used. However, in order to reduce the chances that an anomalous reading will be included in the individualization, a preferred embodiment uses a higher ordered minimum, such as a second or third ordered minimum. Naturally the higher up in this ordered sequence the minimum value is, the more likely the value will yield false negative.

In one embodiment of the present invention some of the features are globally weighted more than others during authentication. A particular feature, such as the slope of the dicrotic notch, may be considered more or less reliable as an identifier and thereby may be given more or less "statistical" weight in the individualization process. Likewise, the correlation between two measurements for a particular feature or the correlation between two different features may be stronger than for other features and be weighted accordingly. Some of the features may carry much more significant information than other features.

During the initial individualization process, it is preferable if the heartbeat signal captured is the first full heartbeat that occurs after the user has placed his finger on a device. The process preferably takes one second or less. In one embodiment, the biometric measuring hardware is primarily an analog circuitry and takes about one-half second before it is ready to begin sampling a user's heartbeat. Because of hardware limitations in some embodiments, heartbeat signal capture within two or more heartbeats is preferable.

The captured waveform is characterized and measured using various predetermined features of the waveform signal from an authenticated user. Based on these preselected features and parameters, individualization data sets are prepared, establishing parameters for each one of the features. The parameters for the features are then used to evaluate heartbeat signals during subsequent authentication. In other words, the present invention determines the likelihood or probability that a particular biometric waveform was generated by the authenticated user. Because the waveform measurements are never exactly the same from sample to sample, the present invention evaluates the probability that two waveforms come from the same person. For each authenticated waveform data sets, a threshold probability value is established for the purposes of authenticating the signal and for use of the signal as a biometric identifier. The threshold value is used to determine whether a specific user's waveform is considered authentic. The threshold may be any value that reflects the desired balance between consistency and selectivity.

One advantage of this embodiment of the present invention is that it takes into account that on occasion a typically consistent feature is [illegible] be inconsistent with its usual pattern. The present invention is able to take such irregularities into account and still provide an authenticating process. For example, if a waveform has an abbreviated peak for some reason, that particular feature that represented the crown of the peak could be lost or unavailable for purposes of authentication. However, with the waveform individualized in accordance with the present invention, there are other features in the individualization set that are still reliable and those other features can accurately authenticate the user. An irregular feature may lower the probability of a positive authentication, but might not lower the probability to the point of giving a false negative. The user may be "recognized" and authenticated from the other features.

After individualization, it may be determined that some of the measured features of a user's waveform are not helpful in the identification process. In other words, for reasons of inconsistency or for other reasons some of the features may not provide information that can be included in individualizing the waveform. In one embodiment of the present invention, features which are not helpful in the individualization process are thereafter not determined or measured during any subsequent authentication procedures for that user. In another embodiment, the features are determined and measured but are not included in calculations or analysis of subsequent waveforms for authentication. By "turning off" the less helpful features, the biometric marker is more succinctly defined. During authentication, the stored memory of a device contains the user's individualization waveform set and only evaluates those particular bivariate and those particular features. Likewise, in another embodiment, in a pre-selection process based upon the relative weights and probabilities of various univariates and bivariates, certain features are flagged as being features that most clearly authenticate an individual. The flagged features are used as the authenticating features for the individual.

In one example the device authenticates a user based upon the user's selecting a user name or identification that is associated with a particular individualized waveform. In particular, the user activates the device which then prompts the user to select from among several registered users, or asks the user to identify himself. The user enters some form of identification recognizable to the device, such as entering or selecting a name, social security number or password, and the device recalls from machine memory the individualized waveform associated with the identifying entry. The machine then takes the waveform of the user and compares it to the waveform recalled from memory. If the waveforms correspond appropriately, the user is authenticated.

Alternatively, a device may be designed to provide access to twenty authorized their individual templates or waveforms and a chip inside the device would store the waveforms or a remote database could store it and the device could access the database. The device then reads the waveform of potential users and interrogates the chip to compare the new waveform to the twenty waveforms stored in the device. If there is a match, the user is granted access. By the same system, the device can determine and keep track of who has accessed the device.

If a particular feature does not match the individualization values, this lowers the probability of generating a true positive. However, for the particular value there is also a range of probable values and based on these calculated probabilities.

The method of the present invention is carried out by being programmed in machine readable instructions, such as is common with computer software, and implemented to act on a computer system. The machine readable instructions may be integrated into a memory chip, or may be stored as data on a portable storage medium such as a floppy disk or CD ROM. The method may likewise be carried out using a signal transmitted over a wired or wireless network where, the signal carries the machine readable instructions.

The present invention may be embodied in other specific forms without departing from its spirit or essential characteristics. The described embodiments are to be considered in all respects only as illustrative and not restrictive. The scope of the invention is, therefore, indicated by the appended claims, rather than by the foregoing description. All changes which come within the meaning and range of equivalency of the claims are to be embraced within their scope.

Calibration Over Time

The method of the present invention comprises obtaining an authenticated biometric measurement. The measurement is authenticated by a process of comparing actual measurements to stored biometric measurements which represent the authenticating data set or template. The template may include specific values for biometric markers or ranges of values for biometric markers. The authenticated biometric measurement must have values that match or fall within the range of the authenticating values of the template. Optionally, the authenticated biometric measurements can be stored separately from the template in machine memory.

The authenticated biometric measurements are weighted and averaged or integrated into the template. By averaging the authenticating measurements into the template, the template can be altered to more closely match the authenticating biometric measurements. Preferably, the authenticating biometric measurements are weighted in order to determine how much of an effect the actual biometric measurements will have when they are averaged into the template.

In one preferred embodiment, univariate and bivariate biometric markers are weighted by assigning each marker a multiplier. A multiplier may be a mathematical function that is used to alter the authenticating template values. For example, a numeric value might be weighted by multiplying the numeric value by 0.001 before integrating the value of the authenticating biometric marker into the authenticating template.

Mathematical equations, functions, or values can be used to weight the authenticating biometric measurements. These equations, functions and values may be adapted as necessary and will differ depending on the type of biometric measurements taken and on the template or authentication data set used. Another criterion used to weight the authenticating biometric markers for inclusion in the template is whether the measurements are known to change in a particular way over time. Knowledge of such changes provides the opportunity to vary the weighting equation or value in a way that anticipates those changes.

Another criterion that may be considered in weighting an authenticated biometric measurement is whether a particular measurement fluctuates regularly. For example, over time it may be shown that a particular biometric measurement has a wide range of fluctuating measurements. Thus, the fluctuations may not be indicative of any particular permanent change and are as likely to affect the values in the template one way as another. To account for this fluctuation and prevent it from undesirably effecting the template, the authenticated biometric measurements of that particular marker or value can be given little or no weight when the authenticated biometric markers are averaged into the template.

The weighting values or multipliers themselves may be changed over time where such adaption is shown to be beneficial. For example, if the authenticated biometric measurements are stored separately from the template, and the values in the stored authenticated biometric measurements indicate a particular value is consistently different than the usual biometric readings, that biometric value may be assigned greater weight than it was initially assigned, in order to account for the apparent pattern of change. Such adaption could allow "bad" initial readings that form an authenticating template to be self-corrected and thereby reduce poor performance or false negatives. Additionally, if the stored authenticated biometric measurement indicate a distinct trend authenticating measurements can be weighted to adjust for a trend in differing values. Likewise, if a particular stored authenticated biometric measurement is stored and later compared with measurements and the template, the weighting of that particular biometric measurement can be changed accordingly.

Calibration itself as a whole may be adapted according to the frequency of use or the number of uses of the system. The authenticating biometric values may be given greater or less weight depending upon the frequency of use or number of uses.

In a preferred embodiment of the present invention, an infrared light is directed toward a specific part of a user's body, preferably the user's finger in order to acquire and store the user's heartbeat signal that can be calibrated to function as a biometric marker. The infrared light of the device penetrates the skin of the finger and is absorbed or reflected off the user's skin and subskin tissues and, specifically, arterial tissues. The reflected light is then received by the system and converted into an electronic signal, which can then be stored in some electronic format and calibrated for biometric authentication.

In this preferred embodiment of the present invention, a series of waveforms are initially measured and stored in an electronic form in a computerized device. The stored waveforms can then be normalized and used to generate a biometric marker template for authentication. The template is later compared to measured waveforms from subsequent users, and, based upon the statistical comparison between the template and the measured waveform, the subsequent user is granted or denied access to a device or authorization for transaction. As the wave form changes over time, the template is calibrated by averaging the authenticating measured waveforms into the template, using a weighted average.

The means for measuring, recording, and storing the waveform employed in the present invention may be any suitable means known in the art, to the extent that such means also allow for calibration of the waveform over time as disclosed and suggested herein. For example, measurement means includes measuring various levels of absorbed or deflected light rays, and electrical impulses and may further include but is not limited to devices capable of measuring pressure differentials, temperature changes, movement, distance, frequency, magnetics, physical interactions and luminescence.

One embodiment of the present invention comprises a device for capturing and calibrating a heartbeat wave form comprising a signal transmitter and a signal receiver communicating with a computer processor and machine memory. The signal transmitter transmits energy into dermal and subdermal tissues of the user of a biometric authentication device. The energy transmitted is partly absorbed into the tissues and partly reflected by the tissues. The signal receiver captures the reflected energy and reflection of the signal. For the purposes of calibration several heartbeat wave forms are collected and stored. The signal data may be collected over any length of time reasonable for authentication purposes. At least one aspect of the data received represents a constant and repeatable characteristic or feature of the signal as absorbed and reflected by the tissues. Furthermore, at least one of the constant and repeatable characteristics is a characteristic that is substantially unique to each person. Preferably, multiple repeatable, relatively consistent features are measured. The resulting constant, repeatable, and substantially unique measurements are calibrated as explained below and are used as a biometric authenticator.

Anticipating that the physiological and anatomical attributes of a user of the present invention will change continuously over time, the present invention provides for a method of ongoing calibration or self-calibration. Self-calibration allows the calibrated, authenticating heartbeat signal or waveform to be modified to coincide with the changes in the user's physiological and anatomical attributes over time. For example, if the authentication system involves monitoring cardiovascular function, the user's heart function changes with time and the signal received from the authorized user may also slightly change over time. Thus, the authorized user's signal may be slightly different form the originally calibrated, authenticating signal.

In order to allow for the changes that occur in the user's body, the authentication program of the present invention provides for some degree of variance between the stored, authenticating biometric marker and an authorized user's waveform as measured at a given time. The program can track such variances over time and recalibrate the authenticating waveform to more closely match the slightly changed waveform of the authorized user, if necessary. Self-calibration allows the authenticating set of measurements (the template) to be recalibrated only within a statistical limit, to more closely match a gradually changing waveform of an authorized user. Thus, as small and insubstantial changes in the authorized user's waveform increase over time, the authenticating signal can also be changed. Self-calibration may be an automatic and continuous calibration that is performed upon each use of the authentication device or may occur at periodic intervals using recalibration data stored up during the period.

In another embodiment, over time, every time a person's waveform is measured and the waveform is authenticated, the values of the particular waveform are stored as part of an ongoing calibration process. The values may be incorporated into the existing authenticating set of marker measurements, but given little weight. Over time, if the authenticated waveform continues to be slightly, but consistently different from the actual calibration will allow the device to continue to be used even though the authorized user's body is changing. For example, if a user's arteries begin hardening, the template would slowly adapt to situations over time, after a thousand or a hundred different ongoing authenticated waveforms are averaged into the template using a weighted average. If a user undergoes a dramatic, sudden change in body function, such as surgery or some form of aggressive therapy, total reprogramming of the authentication set or template may be required.

Layering

In another preferred embodiment, the present invention provides a biometric authentication system that uses a single chip technology to measure multiple, varied biological or histological traits. At least one of the biological traits is a trait that is substantially unique–but not necessarily inherently totally unique (e.g., as in the way that a fingerprint is inherently completely unique to each individual)–to the population of individuals. Although the latter biological trait, herein sometimes referred to as a "first" biological trait, need not be an inherently unique identifier, the latter biological trait is preferably chosen so as to be one that generally remains relatively consistent over time.

In the preferred embodiments of the present invention, a first biological trait is a live physiological trait such as a heartbeat such as that shown in Figure 11. Preferably, the heartbeat is measured so that various features of the waveform can be used to identify the individual whose waveform is being analyzed. For example, the position on the upslope of the heartbeat waveform having the fastest rate of change slope can be recorded and various attributes of that position can be noted. The amplitude of that position, its position from the center of the pulse and amplitude of the actual beat relative to the position can all be measured and recorded. Thus, multiple quantitative features can be extracted from a single characteristic of a waveform.

The heartbeat waveform can also be analyzed relative to the major peaks such as the two peaks shown in Figure 11. Various parameters associated with waveform peaks include, but are not limited to, the differences between the two peak amplitudes, the differences between the two peak rate of changes, the relative position of the dicrotic notch, how deep the notch is, how far the dicrotic notch is from a zero point or from a reference point, and how far the dicrotic notch is from the center of one of the peaks, where the peak of the dicrotic notch is located along the horizontal, and the position of the various peaks from the center of the waveform and from the center of the other peak.

In the preferred embodiments of the present invention, at least one of the biological traits is converted into a digital signal that is signal processed to enhance the of a heartbeat waveform, the captured waveform may be filtered and normalized as shown in Figure 12. In some embodiments of the present invention, some of the quantitative features are globally weighted more than others during normalization and authentication. For example, a particular feature, such as the slope of the dicrotic notch, may be considered more or less reliable as an identifier and thereby may be given more or less "statistical" weight. Likewise, the correlation between two measurements for a particular feature or the correlation between two different features may be stronger than for other features and be weighted accordingly.

The present invention also employs at least a second biological trait that is used in conjunction with the first biological trait (note: the terms "first" and "second" do not necessarily refer to a chronological order) to provide the biometric authentication of the present invention. This second trait is preferably also a live physiological trait–i.e., a trait measurable only on a living individual (e.g., a fingerprint is not a live trait since it can be measured from a dead individual or tissue)–that is substantially unique to that individual.

Examples of live, potentially substantially unique biological traits include the depth of the various layers of epithelial tissue from a given point on an individual's skin surface. The density of a particular kind of connective tissue, such as bone density, may be another substantially unique histological trait. Likewise, the light absorption characteristics of skin tissue or the visual retinal patterns of an iris could be substantially unique histological traits.

In the preferred embodiments of the present invention, the biometric authentication system is designed to operate on a portable computerized device such as a PDA or cell phone. Figure 13 shows an embodiment of the present invention wherein a portable device includes a single computer chip operably connected to a light emitter and detector. In this embodiment, an infrared light (IR) transmitter transmits an IR signal into a person's finger when the finger is placed on the transmitter (whether for purposes of enrollment or verification). The signal transmitter is activated and a signal is emitted from the signal transmitter and is transmitted into the dermal and subdermal tissues of the person's finger. The signal is partly absorbed and reflected by the dermal and subdermal tissues. The reflected signal is received by a signal receiver and transmitted through receiving wires to a chip where the received signal is processed.

Another biological trait is captured in conjunction (whether simultaneously or subsequently) with the first biological trait. For example, in the case of the first trait being a heartbeat waveform measurement taken by using an IR signal that is reflected off of skin tissue, a convenient second biological trait might be the measurement of the aspects of the biological traits is derived from a measurement taken by reflecting light off of the subdermal layers of skin tissue.

After at least two biological traits are measured, the present invention compares each of the traits to corresponding traits previously enrolled for that individual. If both of those traits match their respective enrolled traits, then the individual in question is authenticated.

In some embodiments of the present invention, an individual is authenticated when the individual selects a user name or identification that is associated with a particular biological trait such as a normalized waveform. In other words, the biometric traits may be used in conjunction with non-biometric security features such as passwords, social security numbers, ID cards, etc. For example, the individual or user might activate a portable device of the present invention. The device then could prompt the user to select from among several registered users, or ask the user to identify himself or herself. The user may then enter or select some form of identification recognizable to the device, such as a name, social security number or password, and the device would recall from machine memory a previously enrolled normalized waveform associated with the identifying entry/selection. The machine might then measure the user's waveform and compare it with the enrolled waveform recalled from memory. The user is authenticated if the waveforms correspond appropriately.

In some embodiments of the present invention, the authenticating device is designed to provide access to a set number of authorized users. The authorized users would each enroll their individual biometric traits to be stored in a database either inside the portable device or in a remote database that the portable device can access. When a user desires to be authenticated by the portable device, the device scans the trait database and compares the user's presently read trait with the enrolled traits to find a match. If there is a match, the user is granted access.

Some systems of the present invention include means for verifying physiological activity. These means for verifying physiological activity are primarily to prevent an unauthorized person from using dead tissues as a way to circumvent the authentication process. For example, one device involves a personal biometric authentication system wherein inherently specific biometric parameters are measured and recognized and at least one non-specific biometric parameter is recognized and compared with physiological norms. Likewise, one device involves an anti-fraud biometric scanner that determines whether blood flow is taking place in the object being scanned and whether such blood flow is consistent with that of a living human. In addition, some embodiments of the present invention can keep track of a history showing who has accessed the authentication device.

What is claimed is:

1. A method of biometric identification comprising the steps of:

transmitting infrared energy toward a user, said infrared energy being partly absorbed and partly reflected by said users body;

collecting said partly reflected infrared energy;

processing said reflected infrared energy to create a biometric profile that is substantially unique to said user;

storing said biometric profile to create an authenticating biometric profile; and

comparing said authenticating biometric profile to a subsequently generated biometric profile.

2. A device employing a biometric access system, said access system being adaptable to changes in a user's biometric over time, said device adapting to said changes by using the steps of:

obtaining an authenticating biometric value from an actual biometric measurement;

weighting the authenticating biometric value,

integrating the weighted authenticating biometric value into an authenticating template.

3. A method in a computer system for individualizing a heartbeat signal for use as a biometric marker comprising the steps of:

acquiring a plurality of electronic heartbeat signals from an individual in an electronic signal form;

for each electronic signal, measuring, a plurality of pre-selected features;

for each of said features, calculating the measurement's average;

subtracting the measurement's average from each of the measurements to yield a centroid value;

calculating a standard deviation of each measurement;

dividing the centroid value by the standard deviation for each measurement to give a quotient value; and

calculating the probability of divergence of each measurement using the quotient value in a T-distribution analysis.

4. A computer readable medium containing instructions for controlling a computer system to individualize a heartbeat electronic signal for use in biometric authentication, by:

acquiring a plurality of electronic heartbeat signals from an individual in an electronic signal form;

for each of said features, calculating the measurement's average;

subtracting the measurement's average from each of the measurements to yield a centroid value;

calculating a standard deviation of each measurement;

dividing the centroid value by the standard deviation for each measurement to give a quotient value; and

calculating the probability of divergence of each measurement using the quotient value in a T-distribution analysis.

5. The computer readable medium of claim 2 where said measurements are made on only one variable per observation.

6. The computer readable medium of claim 2 where said measurements are made on two variables per observation.

7. The computer readable medium of claim 2 where said measurements are made on a plurality of variables per observation.

8. A method of biometric authentication comprising:

reading a first live internal biological identifier of an individual, said first live internal biological identifier being a heartbeat waveform measured by reflecting light off of the subdermal layers of skin tissue on said individual;

reading a second live internal biological identifier of said individual; and

authenticating the identity of said individual if both of said biological identifiers correspond with previously enrolled biological identifiers taken for said individual.

9. The method of claim 8 wherein said second live internal biological identifier comprises the depth of a previously-identified layer of epithelial tissue.

10. The method of claim 8 wherein said second live internal biological identifier comprises bone density.

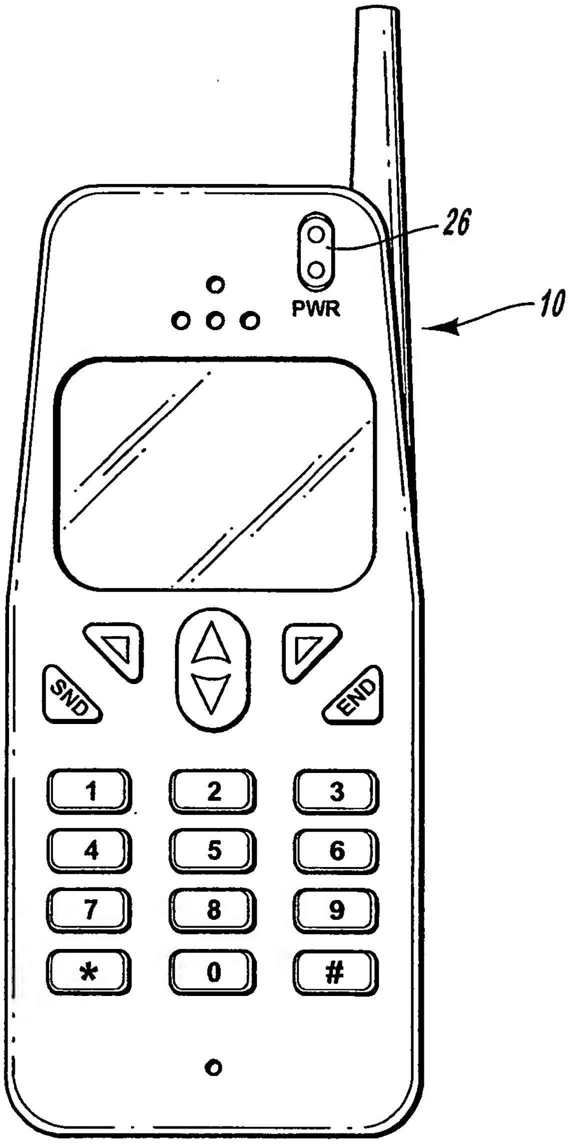


Fig. 1

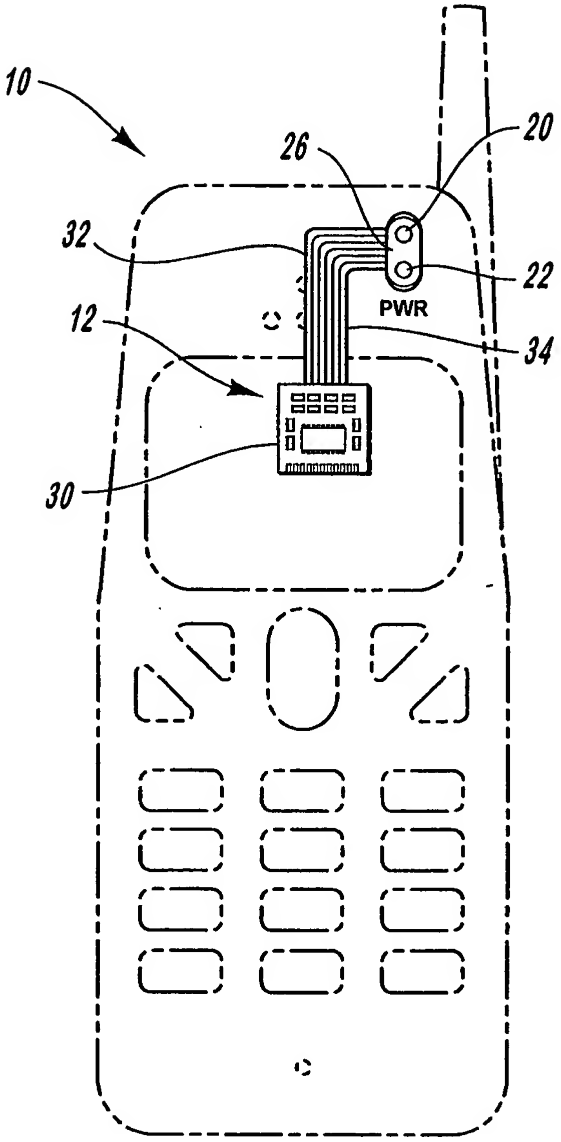


Fig. 2

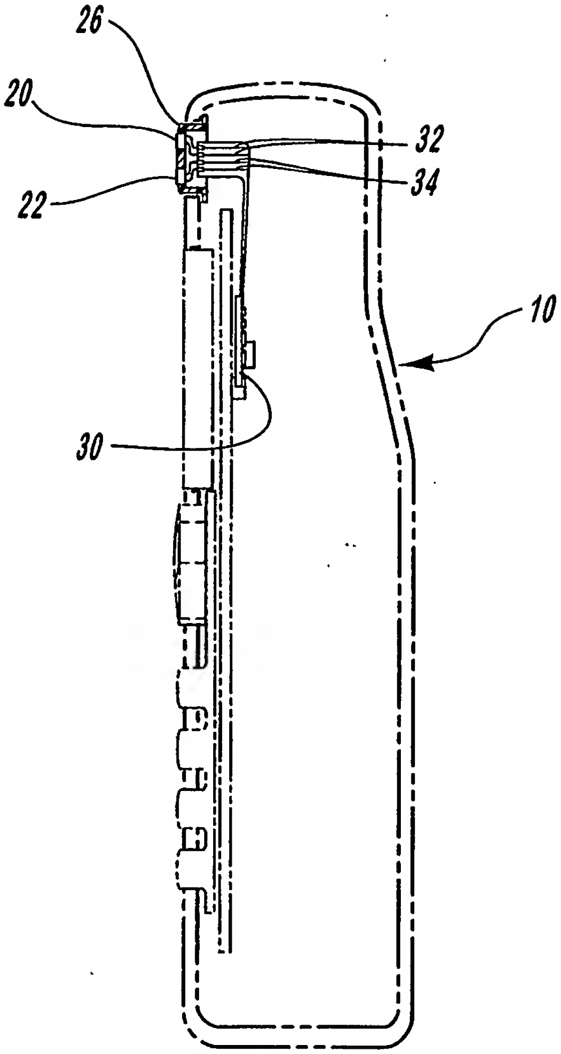
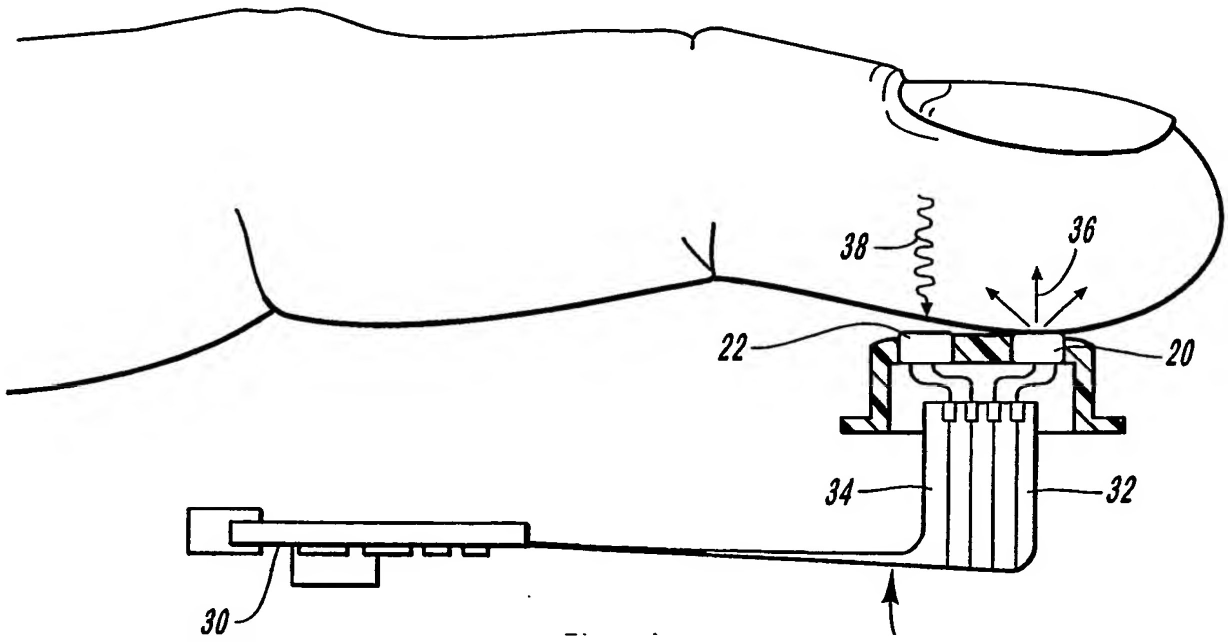


Fig. 3



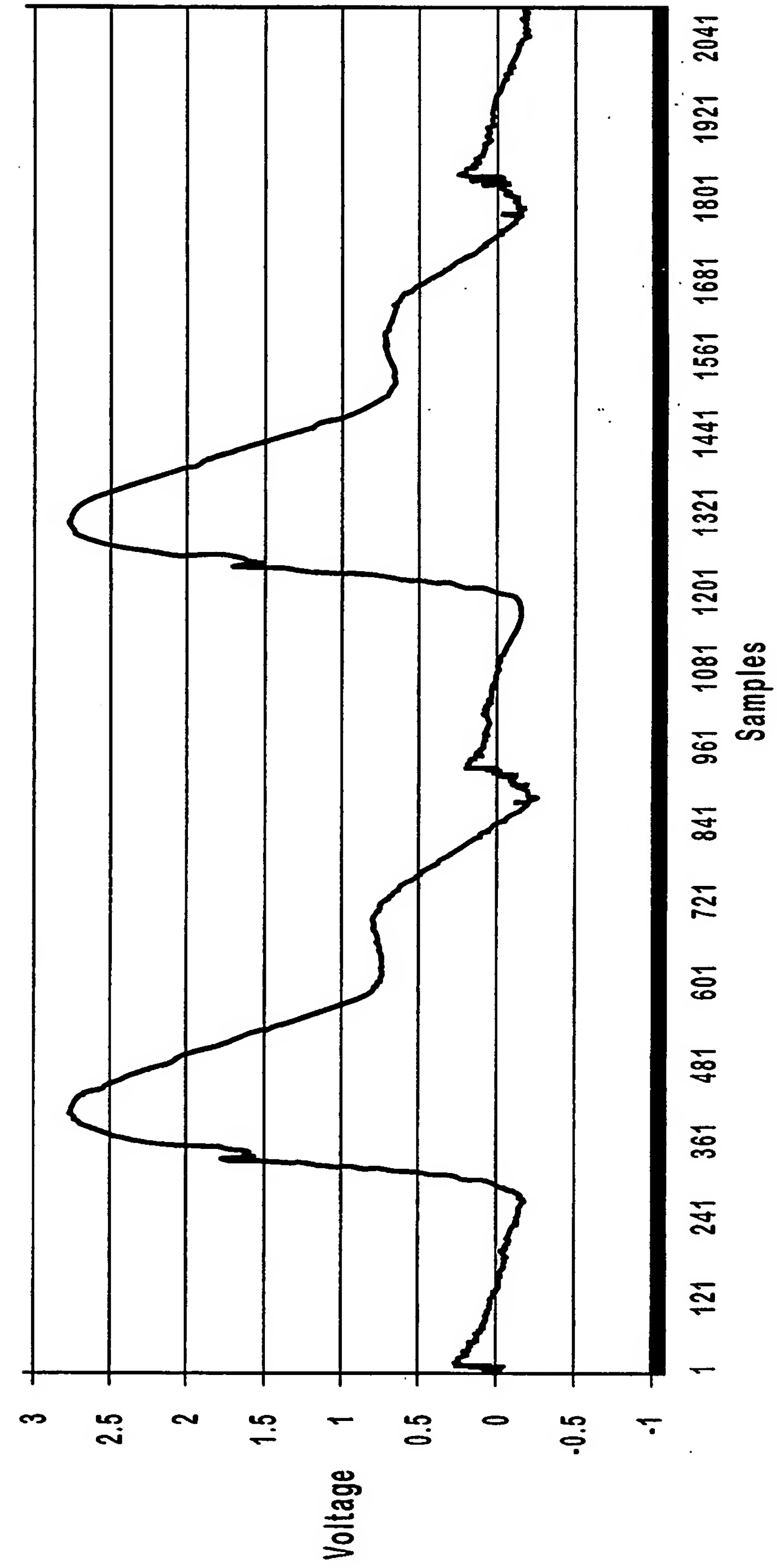

Voltage
3
2.5
2
1.5
1
0.5
0
-0.5
-1
Samples
1
121
241
361
481
601
721
841
961
1081
1201
1321
1441
1561
1681
1801
1921
2041

Fig. 5

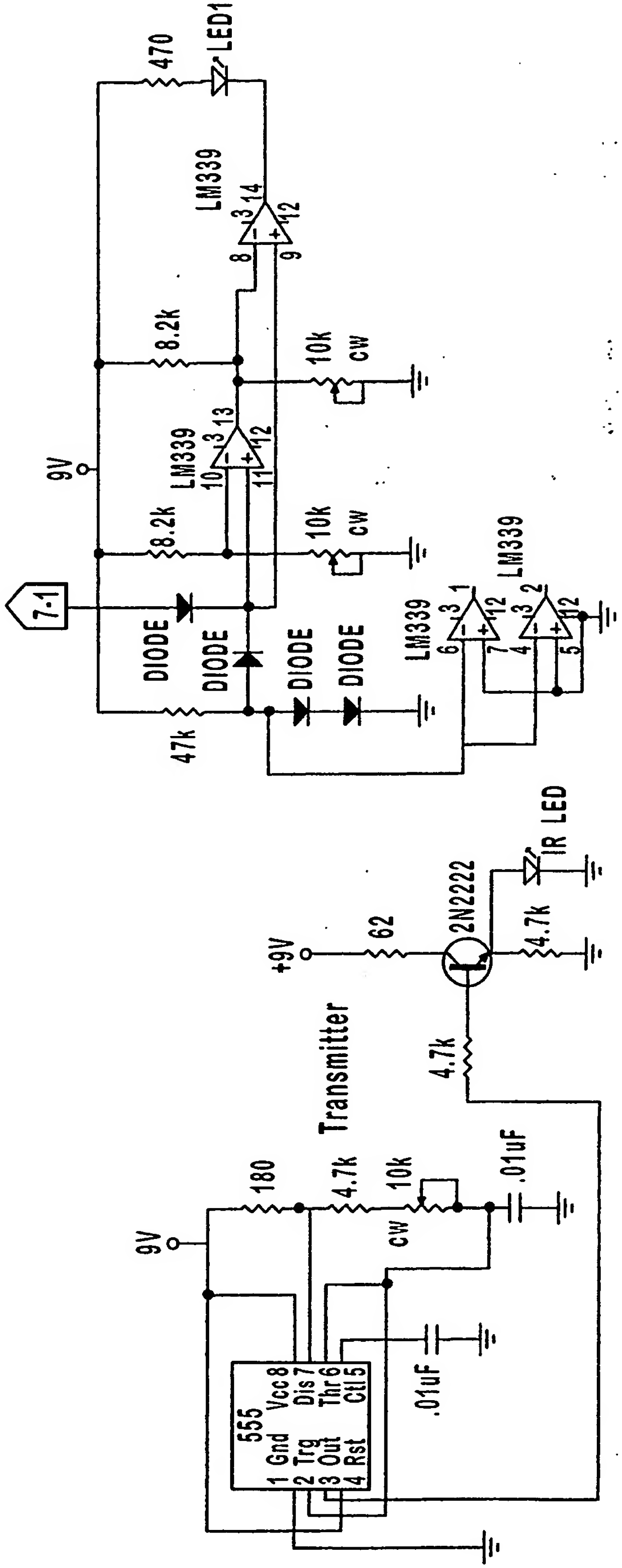

470
LED1
LM339
3
14
8
9
12
8.2k
10k
cw
9V
LM339
10
3
13
11
12
7-1
8.2k
10k
cw
DIODE
DIODE
DIODE
DIODE
47k
LM339
6
3
1
12
7
4
LM339
3
2
12
5
IR LED
2N2222
+9V
62
4.7k
4.7k
Transmitter
180
4.7k
10k
cw
.01uF
9V
.01uF
555
1 Gnd
2 Trg
3 Out
4 Rst
Vcc 8
Dis 7
Thr 6
Ctl 5

Fig. 6

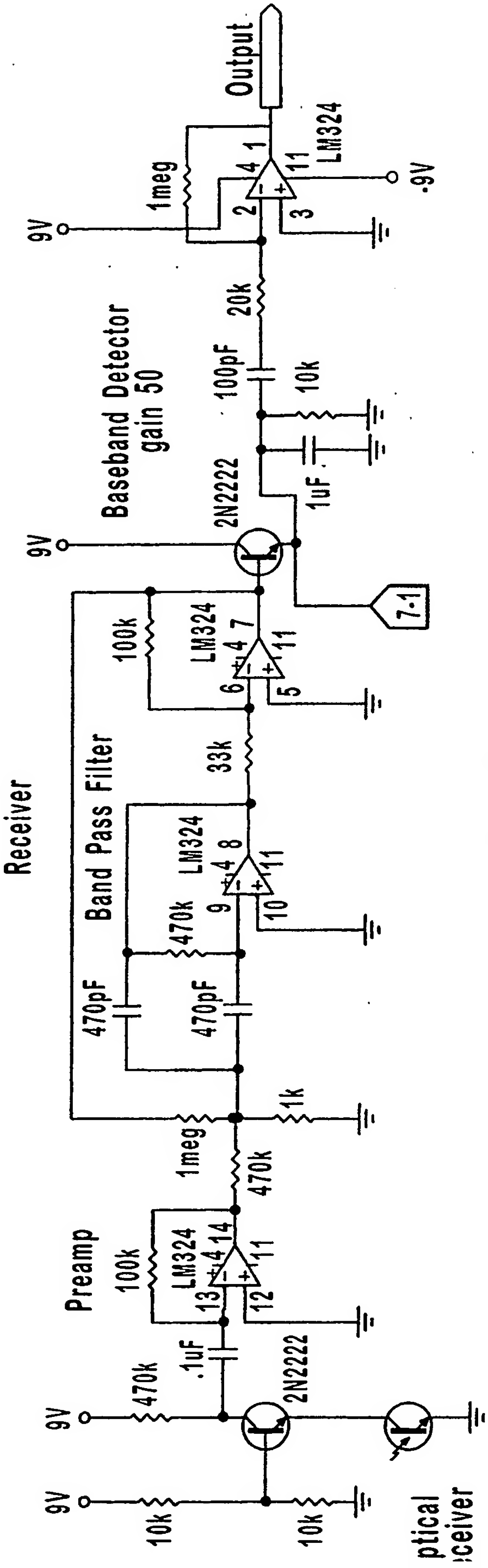

Receiver
Preamp
Band Pass Filter
Baseband Detector
gain 50
Output
ptical
eceiver
9V
10k
10k
9V
470k
2N2222
.1uF
100k
LM324
13
12
4
14
11
1meg
470k
1k
470pF
470pF
470k
9
10
LM324
4
8
11
33k
100k
6
5
LM324
4
7
11
2N2222
9V
7-1
1uF
10k
100pF
20k
9V
1meg
2
3
4
1
11
LM324
-9V

Fig. 7

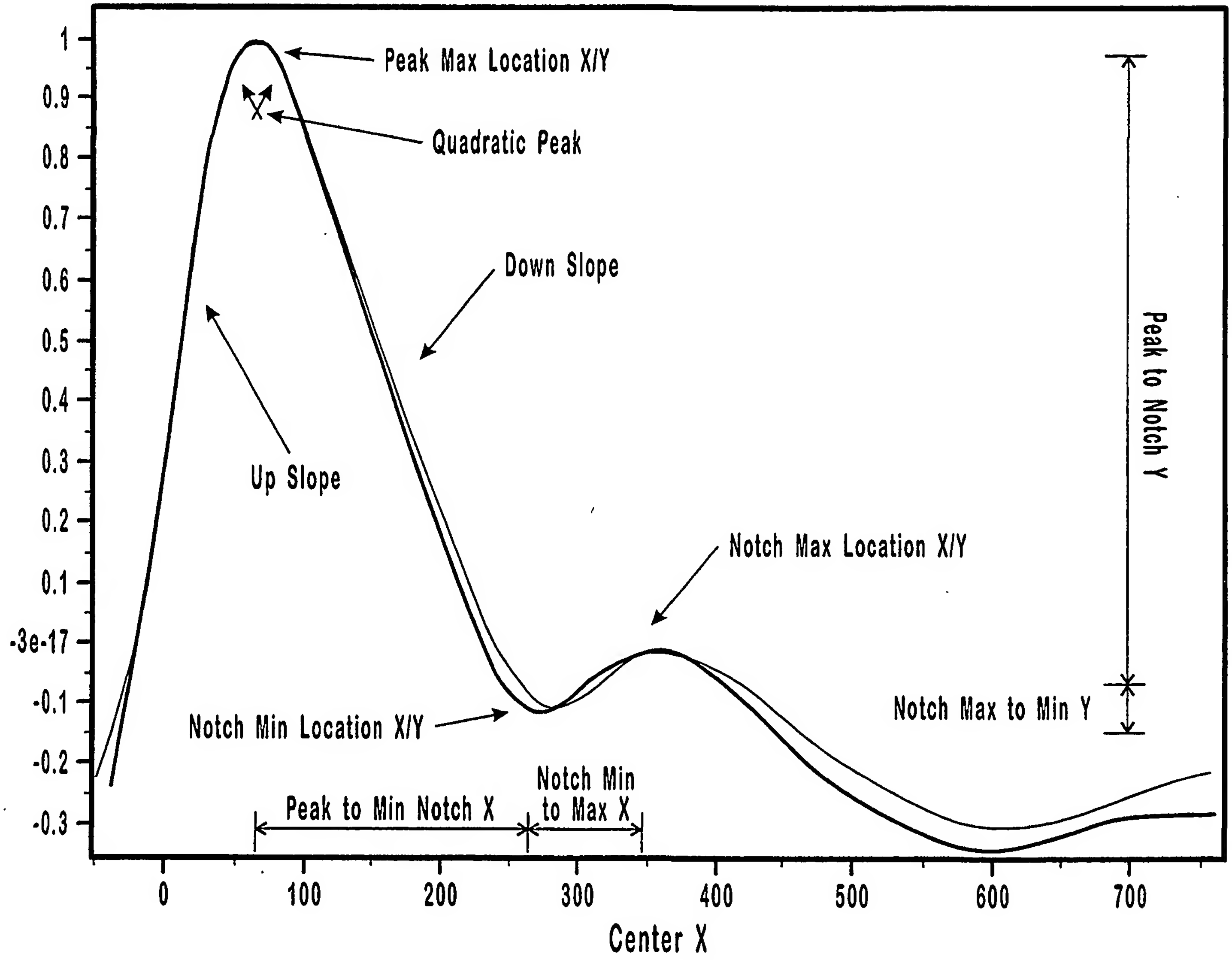

1
0.9
0.8
0.7
0.6
0.5
0.4
0.3
0.2
0.1
-3e-17
-0.1
-0.2
-0.3
0
100
200
300
400
500
600
700
Center X
Peak Max Location X/Y
Quadratic Peak
Down Slope
Up Slope
Notch Max Location X/Y
Notch Min Location X/Y
Peak to Notch Y
Notch Max to Min Y
Peak to Min Notch X
Notch Min to Max X

Fig. 8

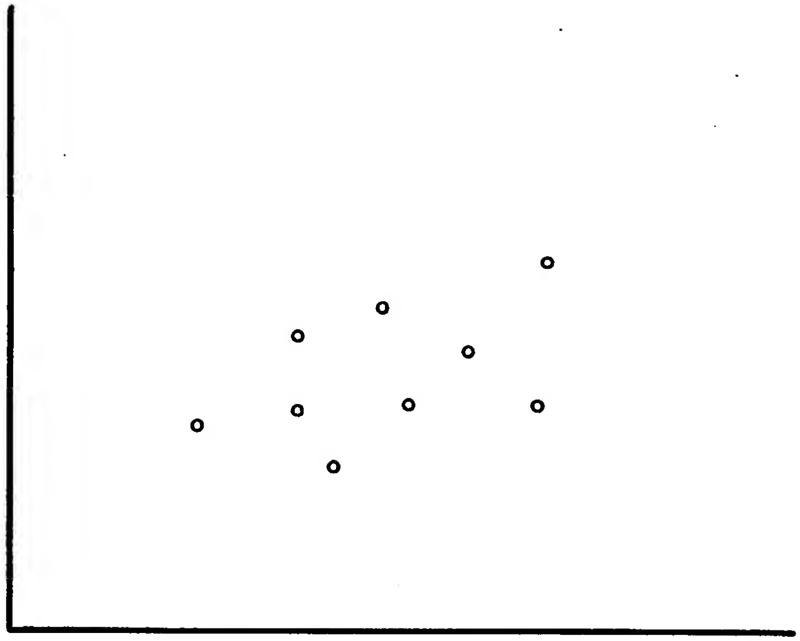


Fig. 9

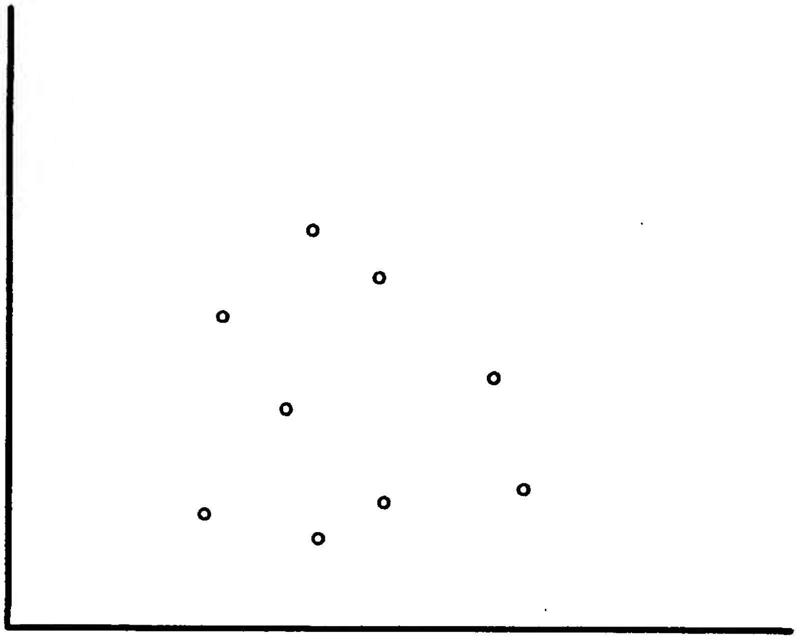


Fig. 10

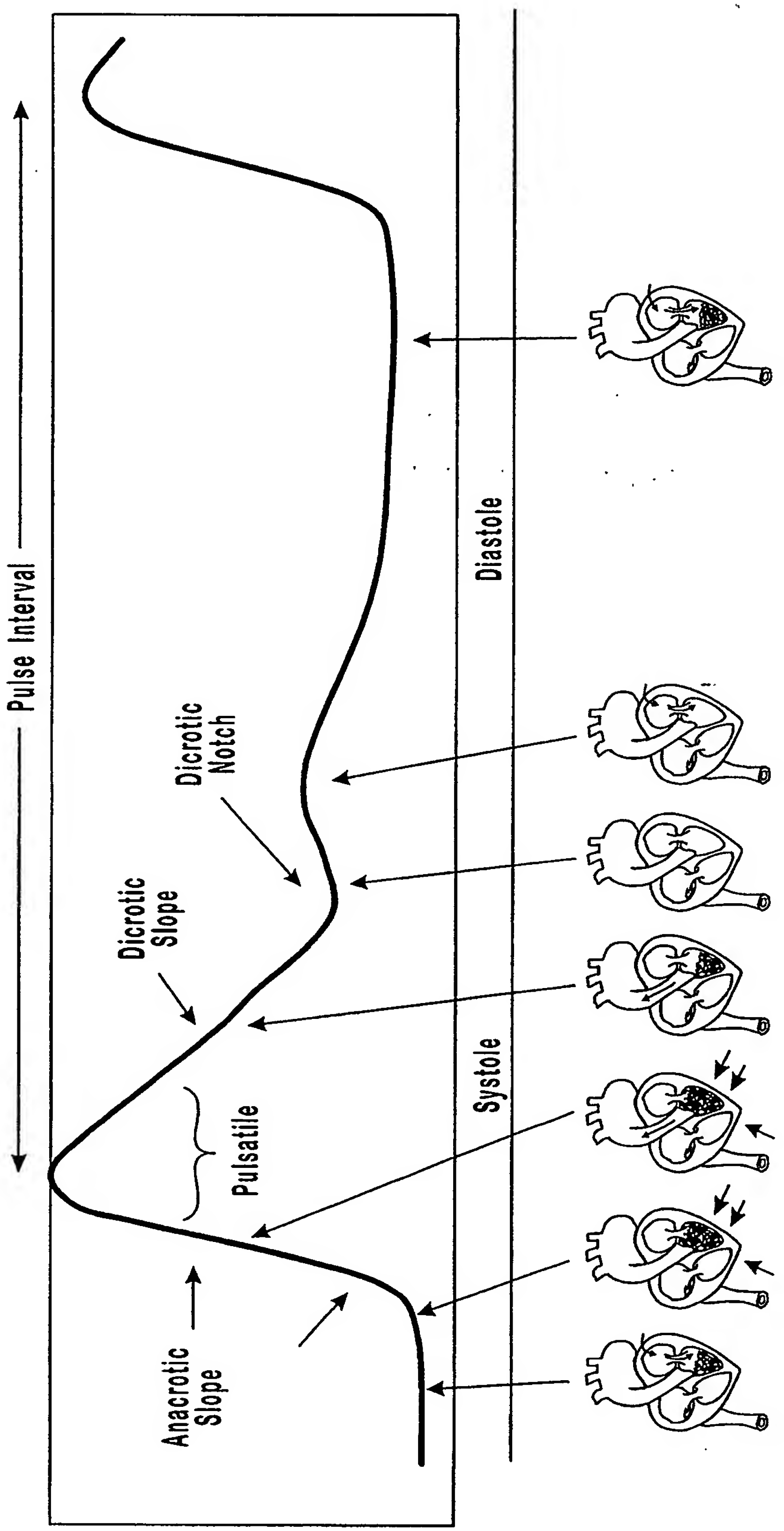

Pulse Interval
Diastole
Dicrotic Notch
Dicrotic Slope
Pulsatile
Systole
Anacrotic Slope

Fig. 11

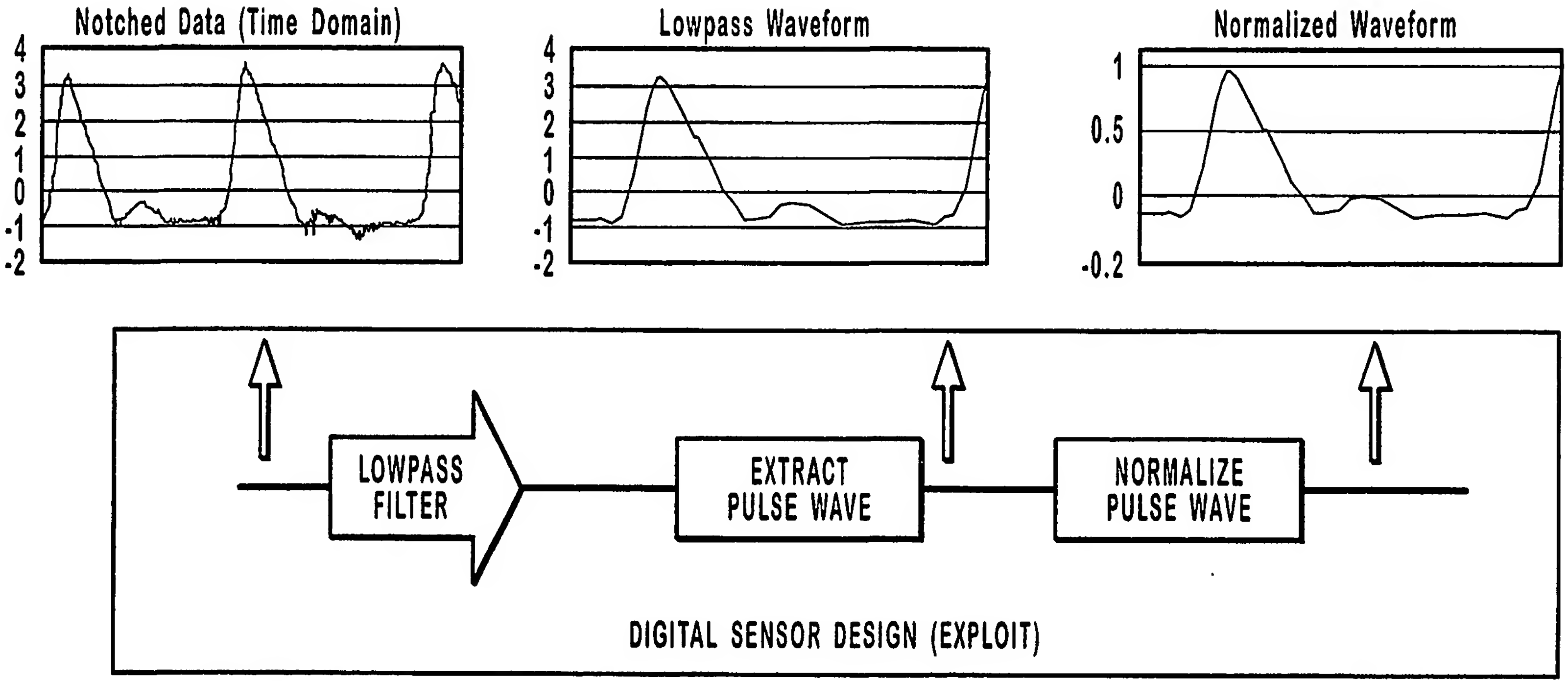

Notched Data (Time Domain)
4
3
2
1
0
-1
-2
Lowpass Waveform
4
3
2
1
0
-1
-2
Normalized Waveform
1
0.5
0
-0.2
LOWPASS FILTER
EXTRACT PULSE WAVE
NORMALIZE PULSE WAVE
DIGITAL SENSOR DESIGN (EXPLOIT)

Fig. 12

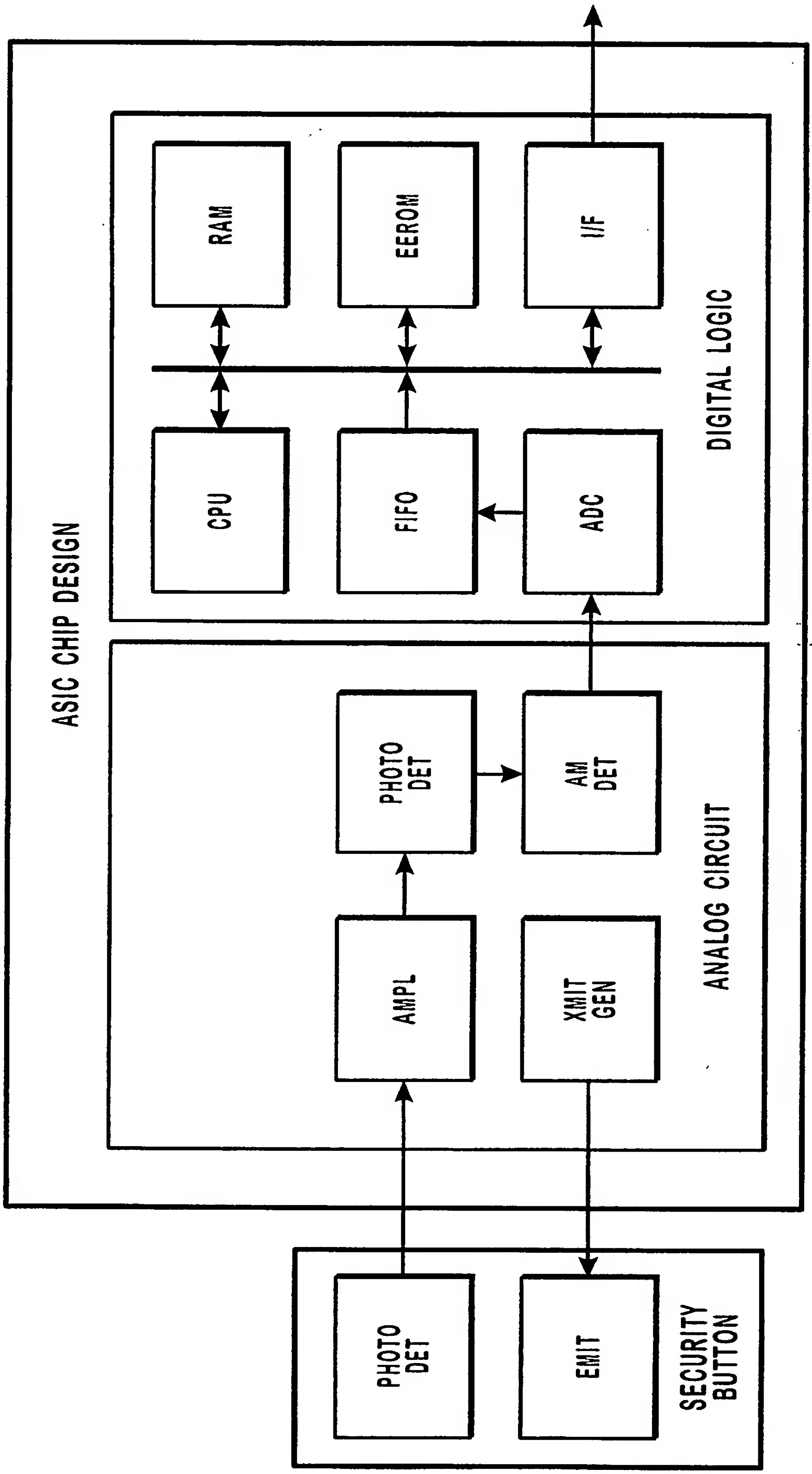

ASIC CHIP DESIGN
RAM
EEROM
I/F
CPU
FIFO
ADC
DIGITAL LOGIC
PHOTO DET
AM DET
AMPL
XMIT GEN
ANALOG CIRCUIT
PHOTO DET
EMIT
SECURITY BUTTON

Fig. 13

INTERNATIONAL SEARCH REPORT

International application No.
PCT/US01/18314

A. CLASSIFICATION OF SUBJECT MATTER

IPC(7) :GO6K 9/00
US CL :382/115, 116; 340/5.82
According to International Patent Classification (IPC) or to both national classification and IPC

B. FIELDS SEARCHED

Minimum documentation searched (classification system followed by classification symbols)

U.S. : 382/115, 116, 124; 340/5.81, 5.82, 5.83

Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched

Electronic data base consulted during the international search (name of data base and, where practicable, search terms used)

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
X	US 5,787,187 A (BOUCHARD et al) 28 July 1998, Figures 1, 2, col. 4, lines 39-46, abstract.	1
Y		2
Y	US 5,982,912 A (FUKUI et al) 09 November 1999, Figure 1, abstract.	2
X	US 5,719,950 A (OSTEN et al) 17 February 1998, col. 2, line 54 - col. 4, line 25.	8-10
A		3-7
A	US 5,737,439 A (LAPSLEY et al) 07 April 1998, All	3-7

□ Further documents are listed in the continuation of Box C. □ See patent family annex.

*	Special categories of cited documents:	"T"	later document published after the international filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention
"A"	document defining the general state of the art which is not considered to be of particular relevance		
"E"	earlier document published on or after the international filing date	"X"	document of particular relevance; the claimed invention cannot be considered novel or cannot be considered to involve an inventive step when the document is taken alone
"L"	document which may throw doubts on priority claim(s) or which is cited to establish the publication date of another citation or other special reason (as specified)	"Y"	document of particular relevance; the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents, such combination being obvious to a person skilled in the art
"O"	document referring to an oral disclosure, use, exhibition or other means		
"P"	document published prior to the international filing date but later than the priority date claimed	"&"	document member of the same patent family

Date of the actual completion of the international search 26 AUGUST 2001	Date of mailing of the international search report 09 OCT 2001
Name and mailing address of the ISA/US Commissioner of Patents and Trademarks Box PCT Washington, D.C. 20231	Authorized officer BHAVESH MEHTA

INTERNATIONAL SEARCH REPORT

International application No.
PCT/US01/18314

Box I Observations where certain claims were found unsearchable (Continuation of item 1 of first sheet)

This international report has not been established in respect of certain claims under Article 17(2)(a) for the following reasons:

1. □ Claims Nos.:
because they relate to subject matter not required to be searched by this Authority, namely:

2. □ Claims Nos.:
because they relate to parts of the international application that do not comply with the prescribed requirements to such an extent that no meaningful international search can be carried out, specifically:

3. □ Claims Nos.:
because they are dependent claims and are not drafted in accordance with the second and third sentences of Rule 6.4(a).

Box II Observations where unity of invention is lacking (Continuation of item 2 of first sheet)

This International Searching Authority found multiple inventions in this international application, as follows:

Please See Extra Sheet.

1. ☒ As all required additional search fees were timely paid by the applicant, this international search report covers all searchable claims.

2. □ As all searchable claims could be searched without effort justifying an additional fee, this Authority did not invite payment of any additional fee.

3. □ As only some of the required additional search fees were timely paid by the applicant, this international search report covers only those claims for which fees were paid, specifically claims Nos.:

4. □ No required additional search fees were timely paid by the applicant. Consequently, this international search report is restricted to the invention first mentioned in the claims; it is covered by claims Nos.:

Remark on Protest

□ The additional search fees were accompanied by the applicant's protest.

☒ No protest accompanied the payment of additional search fees.

INTERNATIONAL SEARCH REPORT

International application No.
PCT/US01/18314

BOX II. OBSERVATIONS WHERE UNITY OF INVENTION WAS LACKING
This ISA found multiple inventions as follows:

This application contains the following inventions or groups of inventions which are not so linked as to form a single inventive concept under PCT Rule 13.1. In order for all inventions to be searched, the appropriate additional search fees must be paid.

Group I, claim 1, drawn to biometric identification using infrared energy.
Group II, claim 2, drawn to device for obtaining authenticating biometric value.
Group III, claim(s) 3-7, drawn to individualizing a heartbeat signal for use as a biometric marker.
Group IV, claim(s) 8-10, drawn to biometric authentication using plurality of biological identifiers.

The inventions listed as Groups I, II, III and IV do not relate to a single inventive concept under PCT Rule 13.1 because, under PCT Rule 13.2, they lack the same or corresponding special technical features for the following reasons: The special technical feature of Group I is the transmission of infrared energy and is not prsent in any of the other Groups II - IV, the special technical feature of Group II is the weighting of the authenticating biometric value and the each of remaining Groups I, III and IV lacks that technical feature, the special technical feature of Group III is the heartbeat signal and that technical feature is not present in Groups I - II and IV and the special technical feature of Group IV is the first and second live biological identifier and that special technical feature is not present in Groups I - III.